Data Protection Impact Assessment

Version 1.0
Authors: Johan Gustav Bellika, Torje Henriksen, Joseph Steven Hurley, Kassaye Yitbarek Yigzaw, Håvard Blixgård
Date: 2018.10.11
Revision history:

<table>
<thead>
<tr>
<th>Issue</th>
<th>Details</th>
<th>Who</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>Initial version</td>
<td>JGB</td>
<td>2018.06.13</td>
</tr>
<tr>
<td>0.2</td>
<td>First draft version</td>
<td>JGB</td>
<td>2018.08.30</td>
</tr>
<tr>
<td>0.3</td>
<td>Revised draft based on input from TH and JSH</td>
<td>JGB, TH, JSH</td>
<td>2018.09.04</td>
</tr>
<tr>
<td>0.4</td>
<td>Revised draft based on input from KYY.</td>
<td>JGB, KYY</td>
<td>2018.09.06</td>
</tr>
<tr>
<td>0.5</td>
<td>Revised document based on input from HB and Guri Rørtveit</td>
<td>JGB, HB</td>
<td>2018.09.10</td>
</tr>
<tr>
<td>1.0</td>
<td>Revised document based on input from the privacy protection team at the university hospital of North Norway.</td>
<td>JGB</td>
<td>2018.10.11</td>
</tr>
<tr>
<td>Section</td>
<td>Title</td>
<td>Page</td>
<td></td>
</tr>
<tr>
<td>---------</td>
<td>-------</td>
<td>------</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Introduction</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>1.1</td>
<td>Summary</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>1.2</td>
<td>Audience</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>1.3</td>
<td>Background</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>1.3.1</td>
<td>Data-flow in the PraksisNett IT infrastructure</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>1.3.2</td>
<td>Extraction of patient data from EHR systems</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>Data Protection Impact Assessment</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>2.1</td>
<td>Systematic description of electronic health record processing operations</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>2.2</td>
<td>Systematic description of processing in the PraksisNett research infrastructure</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>2.2.1</td>
<td>The processing characteristics</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>2.2.2</td>
<td>The extent of processing</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>2.2.3</td>
<td>The context of processing</td>
<td>11</td>
<td></td>
</tr>
<tr>
<td>2.2.4</td>
<td>Prerequisites for processing of patient information on the data reuse server</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>2.2.5</td>
<td>Local statistical processing of patient data on the data reuse server</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>2.2.6</td>
<td>Distributed statistical processing of patient data on the data reuse server</td>
<td>13</td>
<td></td>
</tr>
<tr>
<td>2.2.7</td>
<td>Generating patient recruitment list from patient data</td>
<td>14</td>
<td></td>
</tr>
<tr>
<td>2.3</td>
<td>Purposes of the processing (the legitimate interest pursued)</td>
<td>14</td>
<td></td>
</tr>
<tr>
<td>2.4</td>
<td>Sources, recipients, information security and responsibilities</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>2.5</td>
<td>Assessment of the necessity and proportionality</td>
<td>21</td>
<td></td>
</tr>
<tr>
<td>2.5.1</td>
<td>Principles for data protection / privacy</td>
<td>21</td>
<td></td>
</tr>
<tr>
<td>2.6</td>
<td>The rights of the data subjects</td>
<td>24</td>
<td></td>
</tr>
<tr>
<td>2.6.1</td>
<td>The data subject’s freedom</td>
<td>26</td>
<td></td>
</tr>
<tr>
<td>2.7</td>
<td>Assessment of the risks to the rights and freedoms of data subjects</td>
<td>26</td>
<td></td>
</tr>
<tr>
<td>2.7.1</td>
<td>Measures envisioned to ensure privacy for the patient</td>
<td>27</td>
<td></td>
</tr>
<tr>
<td>2.7.2</td>
<td>New risks introduced by the PraksisNett research infrastructure IT solution</td>
<td>27</td>
<td></td>
</tr>
<tr>
<td>2.7.3</td>
<td>Measures envisioned to address new risks</td>
<td>27</td>
<td></td>
</tr>
<tr>
<td>2.7.4</td>
<td>Measures envisioned to ensure the right not to be discriminated</td>
<td>28</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>References</td>
<td>28</td>
<td></td>
</tr>
</tbody>
</table>
1 Introduction

1.1 Summary

This document contains the data protection impact assessment of the Norwegian primary care practice based research network IT infrastructure, called PraksisNett.

A Data Protection Impact Assessment is a requirement described in Article 35 of GDPR [1] which is introduced by:

"Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks."

This document describes the PraksisNett IT infrastructure in a way that makes it possible for the controllers (the general practice (GP) practices participating in PraksisNett) to perform a Data Protection Impact Assessment (DPIA) of their use of the PraksisNett IT infrastructure. A summary of this report will be used for this purpose. This document has been subject to assessment by UNN’s privacy ombudsman and have been approved by his team of security experts and legal advisors.

The document is based on a checklist provided by the Norwegian data inspectorate [2].

1.2 Audience

Who are the readers for this document?

This document is written assuming an audience of general practitioners, clinical research informatics managers, decision makers, researchers with special interest in how the GDPR requirements are supported by the PraksisNett IT infrastructure.

What background knowledge about the research infrastructure do we assume?

We assume that readers of this document is familiar with the PraksisNett data management plan and how reuse of electronic health record data is done using the Snow system [3]. Interested readers can also benefit from understanding how distributed statistical processing is performed using Snow and Emnet systems [4–6].
1.3 Background

1.3.1 Data-flow in the PraksisNett IT infrastructure

The PraksisNett IT infrastructure contains three types of data resources. That is:

1. Research datasets stored inside GP practice servers (blue barrels in Figure 1)
2. Aggregated and anonymous data generated from all participating GP practices (red barrels in Figure 1)
3. Complete pseudonymised research datasets stored inside safe havens (green barrels in Figure 1).

The orange barrels are the EHR database used daily by general practitioners in GP practices to document patient treatment. Before data can be extracted and stored on the Snow GP practice server (in the blue barrels), the GP needs to consent to usage of the EHR data. When data is stored on the GP practice server, patients can be identified as potential research subject candidates. Data about both patients and health workers stored in the blue barrels are pseudonymized when leaving the EHR server (black arrows). Pseudonymized research datasets stored inside GP practice servers can only be accessed by personnel with access to the Snow GP practice server. Patients can only be re-identified by the general practitioner or by personnel authorized by the general practitioner, from inside the GP practice.

Based on data in the blue barrels, patient data is first aggregated locally at the GP practice and then aggregated across all participating GP practices. This data is stored inside the red barrel, the report database, at the Snow coordinator server. From there aggregated data can be downloaded using a web service interface to the report database. The PraksisNett aggregated data is a subset of the data stored in the snow coordinator server report database. The flow of aggregated data is shown as blue arrows in Figure 1.

The distributed data analysis client, available from the PraksisNett portal, use the data inside the Snow GP practice servers to produce aggregated data, following the procedure explained
above. All results from this processing is stored inside the report database at the snow coordinator server (red barrel) and is available in the distributed data analysis client user interface.

When data collection in a research project is ongoing in the GP practice server, the pseudonymised datasets containing individual patient data will be transferred to the green safe haven. This is shown as the green arrow in Figure 1. The researcher will get access to the complete pseudonymised datasets for advanced data analysis inside the safe haven.

1.3.2 Extraction of patient data from EHR systems

This section is based on the content of [3], which explains in more detail how and what data that can be extracted from EHR systems.

EHR data is extracted from the EHR server using a component we have named “Data reuse component” or DRC for short. This component is run on the EHR server, as shown in Figure 2. The main responsibility of the DRC component is to:

- Replace patient identifiers used in the EHR system with pseudonyms in extracted data.
- Replace general practitioner identifiers in extracted data with pseudonyms.
- Ensure that the same pseudonyms (for each project) are created across collaborating health institutions to allow deduplication of research datasets.
- Ensure that the general practitioner controls whether his patients’ data can be extracted and reused.
- Ensure that patients can be exempted from being identified as potential research subjects.
- Ensure that patients can get information about what purposes their EHR information is used for from their GP.
- Ensure that patients can withdraw from research projects they previously have consented to by contacting their GP.
- Ensure that patients can get their EHR data, which is stored on the PraksisNett IT infrastructure, exported in a machine readable format.

Figure 2 shows the flow of EHR data locally in a GP practice running a local EHR system. Before EHR data can be extracted and stored on the local data reuse server, GPs must approve use of the EHR data by signing a digital approval of data reuse using their smartcards. Data about patients are extracted from the EHR system by the DRC running on the EHR server. Before patient data leave the EHR server, identifiers are replaced with pseudonyms.

The blue lines shown in Figure 2 shows the flow of pseudonymised EHR data. EHR data is first extracted using the data extraction interface of the DRC. It is then stored as an Export file on the data reuse server, and then imported into the Archetype kernel running on the Data reuse server.
When the EHR data is stored in the Archetype kernel it can be analysed by the Emnet local data analysis backend, which supports the PraksisNett client. The local PraksisNett client can re-identify the GP’s patients by calling the Re-identification interface on the DRC. Re-identification is not allowed from the data reuse server. Also, only authenticated and authorized personnel with access to the local area network in the GP practice will be able to authenticate and access the DRC. This is shown as the black arrow in Figure 2.

A research project approved by the PraksisNett board will define the inclusion and exclusion criteria for selecting the patient cohort. These selection criteria will be received by the Emnet local data analysis backend, which will create a local dataset based on the pseudonymised data stored in the Archetype kernel. When a GP has authenticated using the PraksisNett client on his workstation, the list of patients on his patient list can be downloaded to his local workstation from the Emnet local data analysis backend. Within the PraksisNett client he can re-identify the patients by making a call to the re-identification interface of the DRC (black arrow in Figure 2). Only GPs who have valid smartcards and authorized by the PraksisNett will be able to access the re-identification interface of the DRC. We assume GPs may want to authorize local medical secretaries and support staff to access the recruitment lists. These personnel will need smartcards for authentication in addition to authorization from PraksisNett to be able to use the PraksisNett client and re-identify patients using the DRC re-identification interface.
2 Data Protection Impact Assessment

According to GDPR a Data Protection Impact assessment should at least contain (GDPR Article 35, 7):

"(a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;

(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

(c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and

(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned”

2.1 Systematic description of electronic health record processing operations

The systematic description of processing is split in two parts. This section contains a description of processing done using an electronic health record system. As this resource is outside PraksisNett responsibility, it is included for completeness.

How is the information collected?
As described in section 1.3 patient data will be recorded in the electronic health record system used by the GP practice (the orange barrels in Figure 1) as part of medical treatment. The data stored in the electronic health record may also contain information (typically discharge letters) created in other medical institutions like hospitals and emergency wards and transferred to the GP practice electronic health record system using communication software.

How is the information stored?
The patient information is stored in the electronic health record systems. This could be in a GP practice internal server or in servers operated by municipalities or private companies. Some private companies use cloud based storage of patient information.

How is the personal information used?
The patient information is normally used to record medical treatment provided to the patient.

Who has access to the medical information?
In a GP practice, everyone with access to the electronic health record system can normally access all patient information stored in the system. This is necessary to provide medical treatment to the patient. System administration personnel will be able to access the patient information.

Who will be recorded?
Information about patients receiving treatment from the GP.

How can the registered exercise their rights?
Patients can exercise their rights by contacting their GP.

Will there be systematic processing of information about the patients?
Systematic processing of information about the patients may be performed by the electronic health record system.

Are new technology used to process the information?
This is outside our knowledge area as we only have responsibility for processing performed on our data reuse server.

Is the information processed in new ways by old technology that has not been evaluated?
This is outside our knowledge area as we only have responsibility for processing performed on our data reuse server.

2.2 Systematic description of processing in the PraksisNett research infrastructure

This section describes how patient data is processed in the PraksisNett research infrastructure. Patient data stored in the data reuse server will be used for local statistical processing, for distributed statistical processing and for generating patient recruitment lists during the recruitment phase of research. These purposes will be described below.

Section 1.3.1 and 1.3.2 explains the flow of data in the PraksisNett research infrastructure. All processing performed on the data reuse server will be done on pseudonymised patient data. Processing performed on the GP workstation and the EHR server will be done on patient identifiable data. Processing performed on the coordination server will be done on aggregated anonymous data.

2.2.1 The processing characteristics

How is the information collected?
Information stored in the data reuse server is extracted from the EHR using the DRC component. Additional data (typically questionnaires and measurement data) may also be collected as part of research projects and stored on the data reuse server. See also section 1.3.2.

How is the information stored?
The information is stored on the data reuse server, during the data collection phase of research projects. During the data collection phase of a research project, data is also transferred to a secure storage (called a “safe haven”) where the researcher gets access to it. This is only performed for patients that has consented to participation and processing of the information.

How are the personal information used?
The pseudonymised patient information stored on the data reuse server will be used according to the medical record act paragraph 6 (pasientjournalloven), or in research projects.

Who has access to the medical information?
In the GP practice, only the patient’s GP by default has access to the pseudonymised and identifiable patient’s information. The GP may also authorise GP practice staff to access pseudonymised and identifiable patient information. When the patient information is transferred to a safe haven, the principal investigator and the ones he authorises will get
access to the patient information. System administration personnel in PraksisNett and for the safe haven IT solution will have the possibility to access the information.

**Who will be recorded?**

This depend on several aspects; first, only patients that belong to a GP that has signed a digital approval of secondary use, using the PraksisNett research infrastructure. Second, for each individual dataset, only patients that satisfy the inclusion and exclusion criteria of data reuse initiatives will be selected. This can be for research purposes or for purposes that follow the medical record act paragraph 6 (pasientjournalloven). Third, only information about patients that have not reserved themselves from being identified as potential research subjects will be extracted for research purposes. Fourth, only patients that have consented to the use of their information and participation in a research project will have their data transferred to a safe haven.

**How can the registered exercise their rights?**

Patients may exercise their rights by contacting their GP. Patients can avoid being identified as potential research subjects by informing their GP.

**Will there be systematic processing of information about the patients?**

Yes. We envision systematic processing to support the purposes the patient has consented to, and the processing that follows from the purposes described in the medical record act paragraph 6 (pasientjournalloven). For instance, PraksisNett will produce statistics about the patients, their GPs and the consultations covered by the PraksisNett IT infrastructure. PraksisNett will generate statistics about how many GPs that has approved project participation and how many patients that has provided consent to data processing and participation in the research project.

**Is new technology used to process the information?**

Yes. The PraksisNett research infrastructure will process the patient information.

**Is the information processed in new ways by old technology that has not been evaluated?**

No.

### 2.2.2 The extent of processing

**The category of data:** All information stored in the EHR system of the GP practice can be reused. In addition, questionnaire data and measurement data collected in relation to research projects will be collected. The patient must provide consent for all use of the EHR data for research purposes.

**Number of persons:** We envision that the research infrastructure will scale to cover 90 GP practices and 7.5% of the Norwegian population during the first three years. After this period additional funding may enable PrasisNett to scale further.

**Volume of data:** The volume of data is described in [3].

**Frequency of processing:** Processing of the data will be more or less continuous.

**Storage time for personal information:** The research datasets will be stored until it has served its purpose for the research project, that is according to the approval of each research project. This can be many years as data may need to be available for validation purposes when the research has been published. A research project may also need to follow patients over several years.
**The geographical area:** The PraksisNett research infrastructure will cover all health regions of Norway.

2.2.3 The context of processing

In this section, we will examine the processing by looking at internal and external factors that could impact the expectations or the consequences.

**What sources of information will be used?**

We will use information from the medical records of patients, questionnaire, and measurement data.

**What relation exist between the controller and the patient?**

The medical information has been collected as part of medical treatment provided by the GP.

**What is the power relation between the patient and the controller?**

The relation is characterised as a patient – doctor relationship. As the education and experience of a GP within medical subjects normally is much greater than the patient’s, patient would probably accept the recommendation of the GP.

**In what degree do the data subjects control the use of their information?**

The patient has large control over the use of medical information registered about themselves. When invited to participate in a research study, the clinical information that will be used in the research project will be presented to the patient. Based on this information they can detect errors and assess whether they want to support the research project by giving consent. They will be notified about who will get access to the patient information and where the data will be transferred (to a safe haven). They will also be informed about their right to withdraw consent provided to processing of the information about themselves.

**Describe how the processing will be perceived from the patients point of view. Can the processing be seen as unpredictable by the patient?**

As the processing is untraditional, the processing may be viewed as unpredictable by the patient. Efforts will be made to clarify how processing of the patient’s information will be performed. This will be the task of each individual researcher when formulating the study invitation letter and consent forms. The management board of PraksisNett will ensure that sufficient information and clear information will be provided to the patient during the evaluation of the research proposal.

**Do the registered have an expectation of confidentiality?**

Yes. Patients have an expectation of confidentiality.

**Do the registered have an expectation of correct information and a necessity of processing?**

The patients expect that information about them is correct. Information extracted from the EHR for use in the research project will be provided to the patient according to the requirements of GDPR. We believe patients understand the necessity of processing the information for the purposes described in the medical record act and for research.

**Do the registered expect privacy?**

Yes.

**Will the processing include vulnerable persons as children and patients?**
Yes.

Does experience from similar processing exist?
No.

Describe potential progress within technology or security.
The innovation exploited by the PraksisNett research infrastructure is that a privacy preserving system can be used to do statistical computations and locate potential research subject based on the local data storage within GP practices. Only their regular doctor, the author of the clinical information, need to see their records to have the opportunity to participate in relevant research studies.

Does examples of worried voices exist about this method of processing health information?
No, we have not heard such worried voices about this way of processing patient information yet.

Will we process personal information from different sources, collected for different purposes and from different controllers?
Yes. We will also get access to medical information sent to a GP practice from collaborating health institutions. This will typically be discharge letters from various health institutions. Research project may also collect additional data, like medical measurements and questionnaire data which may be stored on the data reuse server.

Will data from several sources be combined to produce new information about the registered?
Yes. We envision combining medical data from several sources. Information from other sources that is stored in the local EHR are discharge letters, test results and evaluations performed by other medical services. It is also possible to envision that data about the patient from several types of health institutions may be combined. For example, data from emergency wards, nursing homes, home care, physiotherapy, hospitals etc. This will improve our ability to get a more correct and complete “view” of the patient’s condition. However, using information from all these institution is not likely to be possible in the near future. However, to ensure validity of this DPIA document beyond the current plans, this vision is included to ensure future validity of this DPIA document.

2.2.4 Prerequisites for processing of patient information on the data reuse server
Before processing of a patient’s EHR information using the PraksisNett infrastructure become possible, a digital approval of participation in a project need to be made by the GP responsible for the patient. When such an approval exists, data can be extracted by the DRC and stored on the GP practice data reuse server. Common to all uses is that a purpose needs to be registered in relation to every dataset that the GP creates. For a research project the purpose will be research. However, every research project must specify its objectives beyond being “research”.

2.2.5 Local statistical processing of patient data on the data reuse server
When a GP has created a digital approval for patient data usage, he can use the local PraksisNett client to create working lists for patient administration, internal control and quality assurance. These working lists can be used for providing health services to patients according to treatment guidelines. Examples include, making a working list of diabetic
patients for regular check-ups, making a working list for elderly that need a flu shot in the influenza season.

2.2.6 Distributed statistical processing of patient data on the data reuse server

Distributed statistical processing of patient data is performed by first aggregating data locally at each participating GP practice. This aggregated data is then aggregated again across participating GP practices (minimum 3 GP practices have to participate) to produce the overall statistical results.

Distributed statistical processing is necessary to perform tasks like research, quality assurance, quality improvement work and disease surveillance. This mechanism makes it possible for GPs to do quality assurance and quality improvement work by comparing their practice to their peers. By having this possibility, they can also participate in quality improvement work and discuss aspects of their practice with their peers. The purpose of this processing is improved medical services for the patients.

An example of such usage is individual GP feedback on their antibiotics prescription practice as shown in Figure 3. The aggregated level (the boxplots) shows the average prescription rates and the distribution across participating GPs combined with the individual prescription rates (the red line).

Similar feedback can be generated for many different areas such as sick leave, referral practice, microbiology testing, drug prescribing in specific medical areas.
2.2.7 Generating patient recruitment list from patient data

For usage of patient data for research purposes, consent from the patient is required, both for processing the patient information and for participation in the research project. Every research project therefore needs to create a recruitment list of patients and send an invitation letter to each potential research subject. The invitation letter text will be prepared by the researcher and must satisfy the requirements from GDPR for informed consent. These requirements are described in article 13 and 15.

The researcher will also define the inclusion and exclusion criteria that will be used to create the recruitment list of potential study participants for each GP that has consented to participate in the study. The GP, which has the responsibility for the potential study participants, will use this recruitment list and the prepared invitation letter and consent forms to create individual study invitation letters to patients. The GP may authorise GP practice support staff to access the patient information and the invitation letter. Information about who has accessed the patient information, who will be accessing the patient information in the future, and where patient information will be transferred after the completion of data collection, needs to be included in the invitation letter and the consent forms. The patient must also be informed about their right to withdraw their consent at any time, their right to get a machine readable copy of the patient data, their right to get a list of persons or category of personnel that have accessed the patient information, and their right to get their data corrected in or deleted from the study dataset.

2.3 Purposes of the processing (the legitimate interest pursued)

What is the purposes of the processing?

The purposes of the processing are: research, patient administration, internal control, quality assurance, quality improvement work and disease surveillance. Every research project also have specific research objectives.

The primary purpose of research is described in the Helsinki declaration article 6 [7] which is:

“The primary purpose of medical research involving human subjects is to understand the causes, development and effects of diseases and improve preventive, diagnostic and therapeutic interventions (methods, procedures and treatments). Even the best proven interventions must be evaluated continually through research for their safety, effectiveness, efficiency, accessibility and quality.”

In addition to usage of patient information for research purposes, patient information can be used for the purposes described in the medical record act (Pasientjournalloven) paragraph 6, which is administration, internal control, quality assurance of medical treatment. Usage of patient information for these purposes enables improved medical treatment of the patients and ensuring that each GP is able to compare his practice to the practice of his peers. Then the GP will have a tool to know whether his practice is within or outside the normal ranges of medical practice. The example shown in Figure 3 shows the “normal practice” as a boxplot visualising the median, 25 and 75 percentiles (the box) in addition to the calculated minimum and maximum.

Paragraph 6 also states that processing for internal control and quality assurance should as far as possible be done without using the name or national personal id number (personnummer) of the patient which is satisfied by the method used in our case.

All purposes listed under paragraph 6 of the Medical record act (Pasientjournalloven), are legal purposes that the Patient cannot object to. Also, processing in relation to asking for consent for usage of the patient information, is within legal uses of the patient information.
Also, as disease surveillance is a task aimed at protecting all citizens and is covered by a specific law that applies to all levels of the health service, the patient cannot deny processing of their information for this purpose.

**Will the information be used for control purposes (such as tax, custom, police or insurance)?**

No. The primary purpose of PraksisNett research infrastructure is medical research.

**Could the purpose be to make decision about individual persons based on systematic and extensive analysis of personal aspects?**

Yes, such usage could be envisioned. However, only after a consent from the patient. For example, patients will be invited to a research project based on a match with the inclusion and exclusion criteria specified by a researcher.

**Will processing of personal information be aimed at decisions that will influence the registered?**

Yes, the intention of research is to improve medical treatment, which will have an influence on patients’ health.

**Will the information be used to profile the registered?**

Yes. The purpose of the research infrastructure is to identify patients that fit the patient inclusion and exclusion criteria of research projects. Also, each GP may wish to find a certain group of patients (like all diabetics) that he wants to follow up on a regular basis.

**Will the personal information be used to uncover unknown traits or to discover pattern of the registered person?**

Yes, such usage could be envisioned, but with consent from the patient. For example, the specific objective for a research project could be to uncover unknown traits and patterns among a group of patients.

**Will the information be processed for other purposes?**

That would be tertiary purposes. No, not without additional consent from the patient. The PraksisNett management board will ensure that all objectives are listed in the consent forms and invitation letters to the patients.

### 2.4 Sources, recipients, information security and responsibilities

**Are all controllers, processors and potential processors identified?**

As the PraksisNett IT infrastructure is currently under construction it is difficult to provide a complete list of controllers and processors. However, Figure 1 provides an overview of the type of institutions that will be controllers of the information about patients. Several potential processors are also identified.

These controllers are:

- **GP practices:** The PraksisNett research infrastructure will recruit 90 GP practices or more to participate in the research infrastructure. Each GP practice will be given a Snow appliance box (a data reuse server) where pseudonymised patient data will be stored. The Snow appliance box will also store questionnaire data and measurement data collected in the GP practices.

- **Safe havens:** When the data collection phase of a research project has started, data belonging
to each individual research project will be transferred to a safe haven. The partial datasets, consisting of the pseudonymised records belonging to the patients that have consented to participation, will be transferred directly to the safe haven. The data will be encrypted during transfer. Two such service currently exists [8, 9].

Processors:

**University hospital of North Norway:** All GP practices will need to sign a data processing agreement (Databehandleravtale) with UNN which has the responsibility for the daily operation of the IT infrastructure. All Snow appliance boxes will be operated using a centralised operation system by the Snow team. Members of the Snow team will be able to remotely log on to each Snow appliance box to do system maintenance. Operation of all the Snow appliance boxes will be logged to a remote and centralised monitoring systems operated by the Snow team. From the Snow appliance box members of the Snow team will be able to log on to the EHR server and do system installation and maintenance of the Data Reuse Component (DRC). UNN can decide to transfer the responsibility for operation of the infrastructure to a third party at any time. Such a transfer will be governed by an agreement that satisfies the requirements from the «The Code of Conduct for information security in the healthcare and care services” and GDPR (Article 28.3).

**Medrave software AB:** As part of the research infrastructure the Medrave tool will be provided to each GP practice. The Medrave tool will extract pseudonymised patient data from the EHR system and use the information to provide feedback to the GPs in the GP practice as part of the quality improvement processes. Personnel from Medrave Software AB will be able to log on to the Snow appliance boxes and do system maintenance on the Medrave installation. Before Medrave Software AB is allowed to install software and log on to any Snow appliance box in PraksisNett a third-party agreement with UNN needs to be made that satisfies the requirements from the «The Code of Conduct for information security in the healthcare and care services” and GDPR (Article 28.3).

**Safe havens:** When research datasets are transferred from the Snow appliance boxes to the safe haven environment, the responsibility of the PraksisNett ends. Agreements will be made with the safe haven responsible organisations before research datasets can be transferred there. Only data about patients that has consented to transfer of their data will be transferred.

Are all recipients of the patient information identified and documented? (employees, data processors, external entities etc)

Two types of patient information will be processed in the PraksisNett IT infrastructure; pseudonymised information and fully identified patient information. By default all employees of a GP practice normally have access to fully identified patient information stored in the GP practice EHR system. The PraksisNett IT infrastructure will become a new channel for accessing the patient information.

**Fully identified patient information:**

Such access is only possible if a number of conditions have been satisfied. These are:

- The GP can authenticate against helseID (must satisfy a number of conditions to achieve this access)
- The GP has approved reuse of his patients’ EHR data
- The GP is authorised by the PraksisNett staff to access the re-identification interface of the DRC from his workstation.
If all above conditions are met, the GP of a patient by default has access to the fully identified record of the patient in a research dataset. The GP may authorise GP practice staff to access the fully identified study research dataset information and the invitation letter, data processing consent and study participation consent form and clinical information overview that will be mailed to the patient as part of the recruitment phase of a research project.

**Pseudonymised patient information:**

By default, all GPs that have approved participation in a research project (by making a digital approval) in a GP practice will be able to access the full pseudonymised research dataset stored in the data reuse server for the GP practice. GP practise staff may also be authorised by the GP to access the pseudonymised dataset.

**How is the patient information shared internally in the practice?**

Fully identified patient data can only be accessed by the patient’s GP, and the staff that have been authorised by the GP. Pseudonymised patient information can be accessed by all GPs that have approved participation in a research project or data reuse initiative (see more details in [3]).

**Which information is shared with whom?**

Datasets are created based on a specification of variables available for extraction from the EHR system (see more details in [3]). Based on this specification a dataset matching the inclusion and exclusion criteria will be created. Before the dataset is created the GP needs to approve including his patients’ records in the dataset. The information in the dataset will be shared according to the description above for internal users and PraksisNett study support staff.

**What is the purpose of sharing access to the patient information?**

The purpose of creating the dataset can be patient administration, internal control, quality improvement work, disease surveillance or research.

**What information is shared externally, for which purposes and on what legal basis?**

Only datasets created for research purposes will be shared externally. In such cases, the pseudonymised dataset is transferred to a safe haven, where it is stored until deleted.

System administration personnel in the Snow team, responsible for operation of the IT infrastructure, may visualise patient information stored on the data reuse server (pseudonymised data) as part of system maintenance through remote desktop solutions.

If Medrave software is installed on the data reuse server, patient information may be visualised through the remote desktop connection to the system administration personnel in Medrave Software AS. These personnel are located in Sweden or Norway.

**Is the information shared with countries outside EU/EØS area on what legal basis?**

No, not according to current plans.

**Will personal information be transferred to third states or international organisations?**

No.

**Describe what precautions have been taken to protect personal information (confidentiality agreements, data processing agreements, norms for information security, security measures).**

- All personnel responsible for system operation of the PraksisNett IT infrastructure
have or will sign a confidentiality agreement.

- All practices that join the PraksisNett IT infrastructure will sign a data processing agreement (databehandleravtale) with UNN, which is responsible for the daily operation of the PraksisNett IT infrastructure. UNN has its own privacy ombudsman, extensive experience within medical research, handling patient information and evaluating information security risks.
- The new Norwegian version of «The Code of Conduct for information security in the healthcare and care services” (which is adapted to GDPR) will be followed.
- Many security measures have been taken to reduce the risk of security breaches to a minimum. They are all described in the “Snow team information security strategy” document. Access to this document is restricted. See also list of additional security measure blow.
- The architecture of the PraksisNett IT infrastructure minimize the risk of information security breaches by design.
- 7 risk assessment processes have been performed so far, both internal and external, covering different aspects of the PraksisNett IT infrastructure.
- Third party processors, like Medrave software AB, which may install software on the Snow appliance boxes to process patient information, must sign an agreement with UNN which states the rights, duties and responsibilities with regard to information security, GDPR (article 28, 3) and the new version of the «The Code of Conduct for information security in the healthcare and care services”.

Additional security measures:

- Each data reuse server is equipped with an on/off switch. The GP practice may stop processing of patient information by powering off the data reuse server, pulling out the power supply or disconnecting the network cable. All these actions will effectively stop the processing of patient information.
- Pseudonymisation. To reduce the risk of exposing identifiable patient information, all data on the data reuse server is pseudonymised. The data reuse server will not contain any information about the identity of patients or health workers. This kind of information will be stored on the EHR server.
- Physical protection of the data reuse server. The data reuse server must be physically protected in the same manner as the EHR server.
- Centralized monitoring. All activities on the data reuse server will be automatically logged to a centralized monitoring system. Persons that attempt to legally or illegally access the data reuse server will be logged to the centralized monitoring system. The centralized monitoring system will regularly produce reports about the activity on the data reuse server. Illegal attempt to access the data reuse server will become visible in these reports. Routines for examining the reports should be established by the GP practices. Then illegal attempts to access the information will likely be discovered.
- Minimizing EHR data extraction. The data reuse server will try to minimize data extraction by extracting EHR data only once per day, preferably in the evening / night, when no one is using the EHR solution. This will minimize the experienced load on the EHR server.
- DRC-software. The available options for installing the DRC software is to install it on the data reuse server or on the EHR server. We have chosen to install it on the EHR server. This will minimize the likelihood of exposing patient identifiable information about patients and health workers and satisfy the requirement from GDPR in the best possible way. However, the solution introduces the possibility of affecting the stability
of the EHR server. A number of measures to minimize the risk of affecting the stability of the EHR server is established.

- Blocking information access from the data reuse server. To eliminate the possibility of getting access to patient identifiable patient information via the data reuse server, such access is blocked.
- Logging of activity on the data reuse server. To expose internal access to patient information all access to datasets will be logged. The activity will be reported regularly as part of the information security report to the GP practice. Legal and illegal access to patient information will become visible in these reports. All system administration personnel will use personal login accounts. All system administration will be logged with a reason for login and will also be reported as part of regular reports to the GP practice.
- Transfer of research datasets. To reduce the risk of losing research datasets (physical loss), datasets will not be transferred to the researchers. The research datasets will be transferred to safe havens where the researchers get access to it in a secure environment.
- Other security measures. A number of other measures to ensure health workers access to EHR information and reduce the risk of exposing EHR information about the patients and the health workers is used. One of the most important ones is following «The Code of Conduct for information security in the healthcare and care services».

Do you have an agreement or contract with external organisations about the mutual understanding and responsibilities?

Yes. All GP practices running a Snow appliance box must sign a contract with PraksisNett that clarifies rights and obligations for participation in PraksisNett.

The GP practice will also sign a data processing agreement with the University hospital of North Norway that clarify the responsibilities of both parties.

Do the agreement reflect the limitations for sharing personal information?

Yes.

The relation to processors, for each processor:

Are all processors identified and is the relation to each one clarified through agreement (article 28,3)?

All planned processors have been identified. These are the Snow team at UNN which is responsible for daily operation of the PraksisNett IT infrastructure, the safe haven institutions (TSD at UiO and SAFE at UiB), the responsible research institutions that the researchers belong to, and third-party vendors like Medrave software AS providing IT support for the quality improvement software tool.

Are the registered right and freedom ensured in the agreements?

Agreements between the PraksisNett consortia and each researcher will need to be made to ensure that the rights and freedom of the registered is ensured. The patient has the right to withdraw his consent for usage of his information in a research project. While the data is stored inside the data reuse server of the GP practice, the GP himself can delete the record in the research dataset using the PraksisNett client. An access log for each dataset (corresponding to a project) is kept at the data reuse server. When the research dataset has left
the PraksisNett research infrastructure, the researcher must ensure that patients that withdraw from a study are deleted from the research dataset. To withdraw from a study, the patient needs to contact his GP which will identify the patient’s pseudonym. The GP will instruct the responsible researcher to delete the record corresponding to the pseudonym in the research dataset. A satisfactory access log needs to be kept by the safe haven. The access log may be provided to the GP in case a patient wants to know who has accessed his pseudonymised data.

**Are the privacy principles, for instance limitation of purposes, data minimisation, storage etc. handled in the agreement?**

Not to a great extent, as it would be too extensive to be described in the agreements. However, the rights of the patients are ensured by the architecture and the functionality of the PraksisNett IT infrastructure (limitation of purpose, data minimisation, data correctness, logging of use, safe storage, ensuing the opportunity to get the data deleted from the dataset, the right to get a copy of the data in a machine-readable format, etc). The agreements state that only patients that have consented to participate in a research project can have their information exported to a safe haven.

**How is the information you share with a recipient secured at the receiving end?**

Research datasets are transferred from GP practices to safe havens (TSD at UiO and SAFE at UiB). As part of an agreement with the receiving safe haven, a description of how security is handled need to be provided.

**What education is necessary for the personnel in external organisations, before they get access to information?**

The safe haven personnel need to know the details of the agreement with PraksisNett. They need to know the GDPR requirements, and how to delete records in research datasets that belongs to research subjects that have withdrawn their consents for participation and use of their information. They also need to know how to store data access and processing logs of research datasets to ensure that a person may request overview of who has used their personal information.

Third-party (i.e., Medrave software AB) personnel need to know the “The Code of Conduct for information security in the healthcare and care services”. They also need to know the requirements stated in the agreement with UNN, which is responsible for processing.

**Does the processor provide satisfactory guaranties for suitable technical and organisational measures that ensure that the processing will be performed in accordance with GDPR (Article 28 1)?**

The data protection team at UNN will assess whether the specifications and the routines of the Snow team is acceptable and provide a recommendation to the GP practices.

For third party processors, performing operations on behalf of UNN, a specific agreement with specific requirements will be made. The third-party processors must satisfy these requirements.

**Are all data flow, storage and temporal storage identified?**

The data flow in PraksisNett is described in section 1.3.1.

*As we have not completed the specification for safe storage of research datasets, all flow, storage is not identified.*

**How is the data transferred and made available (data flow)?**

See section 1.3.1.
Where and how long is the information stored on the specific sources?

Local partial research datasets: The local research datasets will be deleted when the data collection phase is completed and the partial research dataset is stored in the safe haven. Only the access and processing logs necessary to ensure the rights of the registered are kept (the DRC link between personal ID number and project ID and Emnet processing logs).

Research dataset at the safe haven: Dataset at the safe haven will be stored until they have fulfilled their purposes. This include the time needed to ensure that the published research papers can be validated for correctness.

How long is the information stored after completing the purpose of the processing, before the data is deleted?

One day should be sufficient. When the data has fulfilled its purpose, it will be deleted.

When will the information be deleted?

The next day.

Have you developed routines for deleting information?

At the local data reuse server: No, not yet.
At the safe haven: Too early for that.
Safe storage of research datasets: Not yet

Is information security handled satisfactory?

The privacy protection team at UNN has assessed whether the information security is handled satisfactory in the IT infrastructure and given it its recommendation.

Are all active and planned measures suitable to ensure confidentiality, integrity and accessibility of information about persons?

This cannot be evaluated by us.

Are security standards, policies and norms for information security followed?

For our part; yes. For third party vendor compliance needs to be checked regularly to ensure that standards, policies and norms are followed.

2.5 Assessment of the necessity and proportionality

2.5.1 Principles for data protection / privacy

Legal basis

Is the processing lawful, fair and transparent (article 5.1 letter a, and article 6 and 9)?

What is the legal basis for the processing?

- Consent, agreement /contract, legal obligation, vital interests, exercising public authority, legitimate interest?
- Does the legal basis include the purpose of the processing and transfer to externals?

The Snow appliance box is, when installed in a GP practices, part of the controllers (GP practices) responsibility and can be used for all legal purposes that follows from Norwegian law, especially the medical record law §6, which states that the patients’ data can be used in relation to medical treatment, internal control, patient administration and quality assurance of the health service.

The patients’ data on the Snow appliance box is also used for disease surveillance purposes,
which is legal processing with a basis in the disease prevention law (smittevernloven) §7-1 and §7-2 b and e.

For research purposes written consent from the data subjects will be collected for use of the health information and for study participation.

**Have you evaluated and controlled that the purpose is valid and reasonable?**

- What are the expected benefits of the processing? For the organisation, the registered and the society?
- Is there a clear separation between personal information that is necessary for the agreement and what information that need to be based on consent?

The long term expected benefit from the processing and research is improved medical treatment for the patients, the health service and our society. Also, participation in research projects on specific diseases may be assessed as a benefit by the patients. Some patient may claim it is unfair that they cannot participate in research projects, because their GP is not part of the PraksisNett research infrastructure.

Research projects will define the variables that will be used in the research project. Written consent for use of the information will be collected from the patients. The patients will be provided with a copy of the information, to ensure that the information is correct and that the patient is informed about what data that will be used in the research project.

**Assess how transparency is handled in the processing.**

The patient may ask and get information about what purposes his or her data has been used for. If requested, the processing logs of each data reuse project (including research projects) can be provided. When data has been transferred to safe havens, access logs and processing logs may be provided. However, processing performed in safe havens is outside the responsibility of the PraksisNett IT infrastructure.

**Limitation of purpose (Formålsbegrensning)**

The purpose of processing should be lawful, fair and transparent (article 5.1 b). Check the following:

- Is the purpose clearly defined?

The purpose of processing datasets within the PraksisNett IT infrastructure must always be specified. Each research project will pursue its specific objective.

**Is the purpose defined in accordance with the expectations of the registered?**

We assume that patients expect that their medical data is used to provide high quality medical services. The patients also assume that the information is used based on their consent.

**Can the purpose be accomplished using less invading methods?**

All processing in the Snow appliance box is based on pseudonymised data. It is not possible to use anonymous data, as this would prevent ensuring that data subjects can exercise their rights (the right to withdraw consent, transparency of use).

**Can the purpose be accomplished using anonymous or pseudonymous alternatives?**

Yes, pseudonymous data can, anonymous data cannot.

**Data minimisation (article 5.1 c)**

Personal data should be adequate, relevant and limited to what is necessary.
Assess the purpose of processing: Is it possible to achieve the purpose by:

- Limiting the collection of personal information?
- Limiting the level of details of personal data
- Without using secret and sensitive information?
- Using aggregated or pseudonymous personal data?

Assess the necessity and relevance related to the purpose for every variable in a dataset.

The variable set proposed by researchers will be assessed by the management board of PraksisNett as part of the project approval process. As part of this assessment, evaluation of these issues will be performed. Also, GPs will perform the same assessment when consenting to participation in a research project. However, the GP will potentially put a lot of trust on the management board’s evaluation of these aspects.

Correctness (article 5.1 d)

Personal data should be correct and updated

How is personal data kept correct and updated, with or without involvement of the data subject?

Patient involvement: As part of the invitation letter to the patient, a copy of the clinical information used in the research project will be provided. Error discovered by the patient must be communicated to their GP, which should then correct the information in the research dataset or in the EHR (if legal and possible).

Without patient involvement: Automated data quality checks will be used to provide the GP with a tool to improve the correctness of the clinical data stored in the PraksisNett IT infrastructure.

Assess whether necessary functionality exist to correct or erase personal data.

Correcting a medical record may be difficult. We are uncertain whether corrections can be made in the EHR system. Legal advice is needed here. Error in clinical data need to be corrected by the GP responsible for the patient. Information should ideally (if possible) be corrected in the source, the EHR record. If that is not possible, data can be corrected in the data reuse server.

From the data subjects point of view, is there a need for contradiction?

Research subjects will be provided with a copy of the EHR information used in the research project. The research subject / patient may ask the GP to correct errors in the information.

Do the data subjects have the opportunity to object on what controller has registered?

Yes, by using the information provided as attachment to the study invitation letter.

Do you have routines for how employees write journals, memos, minutes etc.?

No, but routines for writing medical record notes may need to have some.

Limitation of storage (article 5.1 e)

Personal data should be deleted or anonymised when the purpose has been accomplished.

Is the personal data kept after the purpose has been accomplished?

When is the data deleted?
When is the personal data pseudonymised or anonymised?

Research datasets that has fulfilled its purposes will be deleted. However, we assume most datasets will be stored in safe havens, outside the responsibility of the PraksisNett. Agreements between PraksisNett and the safe haven organisation will ensure that the responsibility to delete research datasets is placed with the safe haven institution. All data stored on the Snow Appliance box in the PraksisNett IT infrastructure will be pseudonymised.

Safeguards (Article 89.1)

What safeguards must be in place if personal data should be stored for a longer time period for purposes related to archives in public interests, purposes for scientific or historical research or statistics?

Before data can be stored in a safe haven, an agreement need to be made between PraksisNett and the Safe haven. The agreement must state what policies will be used to safeguard personal data and how long personal data will be stored.

The research datasets may need to be stored for some time to ensure that published research can be validated for correctness. However, when research datasets have been deleted in the safe haven environment, a notification should be sent to the GP practices, notifying the GP practices that the specific research dataset has been deleted. If the data subject asks for an overview of what their data has been used for, information can be provided that the specific research dataset has been deleted. As long as such notification has not been sent, the data subjects can get information about where their clinical information is stored from their GP.

Is it necessary or possible to improve the proposed methods of processing?

We don’t think this is possible today. It will always be necessary to improve the processing methods to reduce risk of exposing sensitive data.

The development of distributed secure multiparty computation methodology will at some time in the future remove the necessity of moving research datasets out of health institutions. Datasets can be analysed locally, while ensuring the privacy of patients and health personnel and minimising distribution of highly sensitive information.

Is it possible to improve the condition for the registered?

Only by advancing the distributed secure multiparty computations, as explained above.

2.6 The rights of the data subjects

Assess how the rights of the data subjects is handled:

Assess how information is provided to the data subjects? (article 12,13,14)

The patient will be informed by their GP practice about their rights. They will also be informed about how and for what purposes their EHR data is used, who is able to access it, while stored in the EHR system, on the PraksisNett IT infrastructure, and in safe havens. We assess these efforts to be adequate and reassuring to maintain the trust between the patient and the GP, necessary to get consent for use of the information for research purposes.

When their data is used for research, additional information about how their data is handled, who will access it and where their data will be transferred will be provided to the patient as attachments to the consent forms.

Assess how consent is collected (Article 7 and 8)
Is the consent provided freely and explicitly?

Is the consent documented?

Consent for participation in research and use of personal data will be mailed to the patient. The patient must then sign and return the written consent to the GP practice which will store the consent forms in the GP practice.

Can the data subjects withdraw consent, as easy as giving it?

Yes, patient can withdraw their consent at any time by contacting the GP that invited the patient to participate in the study.

Can the data subjects get insight into personal data?

Yes, the GP will be able to provide the patient with a copy of the data as part of the study invitation letter or later while the research dataset is still stored at the GP practice Snow appliance box. When the research dataset is moved to the safe haven, the GP must notify the safe haven and the responsible researcher for the research project to provide a copy of the pseudonymised data.

Can the data subjects get a machine readable copy of the data? (article 15 and 20)

Yes, the PraksisNett IT infrastructure will contain functionality to extract machine readable data about a specific patient.

Can the data subjects get his data corrected? (Article 16)

Yes, as long as the data is stored at the Snow appliance box. After transfer of the research dataset to a safe haven, the GP must notify the responsible researcher that information in the dataset need to be corrected for the specific pseudonym belonging to the patient. However, this issue is the responsibility of the safe haven institution.

Can the data subjects get his data deleted? (Article 17)

Yes, by contacting the GP that invited the patient. While the research dataset is stored at the GP practice the GP himself can delete the data in the research dataset. When the research dataset is moved to the safe haven, the GP must notify the responsible researcher to delete the data corresponding to the pseudonym of the patient.

Can the data subjects right to restrictions of processing, objections to processing, and right to notification regarding rectification or erasure of personal data be handled? (Article 18, 19, 21)

The patient can reserve himself from being invited to participate in research projects by notifying his GP. The DRC will then remove this person from inclusion in recruitment lists used to recruit patients to research studies.

Are automated individual decision making, including profiling, performed? (Article 22)

Yes, in the sense that patients are selected to be part of research datasets based on inclusion and exclusion criteria specified by a researcher. The GP may also use his local PraksisNett client to identify the patient based on information stored in the EHR system.

What is the legal basis for such processing? Explicit consent or law?

Both legal and consent.

Is it necessary or possible to improve the way the data subject rights are handled?

During the study invitation phase invitation letters, consent forms and clinical information will be provided to the patients through mail. To perform these manual operations, support
staff at the GP practice may be used. An assessment must be made whether such personnel can take part in this process. We need advice on this questions from our evaluators.

2.6.1 The data subject’s freedom

Assess how the data subject’s rights in relation to the European human rights convention is assured?

The right to privacy and net neutrality

The right to privacy has been realised as far as current technology is able to bring us. Advancement on distributed secure multiparty computations can bring us even closer to an environment where the risk of privacy breaches for the patient can be minimised.

We do not see how net neutrality is affected or affect us.

The right not to be discriminated

Patients do not have the right to participate in research on conditions they suffer from. However, they have the right to select their GP and to some extent the health institution where they will be treated. An assessment must be made on whether patients having GPs that do not take part in research studies on the patient’s conditions is a way of discriminating the patients wish to contribute to research on their medical condition.

Freedom of thought, belief and religion

The patient is able to deny participation in research projects that have contact points with his/her strong religious views. Like abortion, vaccines, sexual preferences.

Freedom of speech and information

We cannot see any relation to these issues.

Is it necessary or possible to improve the way the data subject freedom is handled?

It is possible to give more patients in Norway access to participate in research projects on their medical condition. It is also possible to improve protection of patient privacy and reduce the exposure of their medical record data. However, this is a question of funding research within these domains. We assess the efforts described in this document to be adequate and reassuring to maintain the trust between the patient and the GP, necessary to get consent for use of the information for research purposes.

2.7 Assessment of the risks to the rights and freedoms of data subjects

In the sections above, we have described the plans made to ensure the rights and freedom of the registered. In the sections below we will describe the reasoning behind the choices made and how these choices minimize the risks, along with the potential risks introduced by not following them may have for the patients.

The Snow system, which is the basis for the PraksisNett IT infrastructure has been subject to 7 risk assessments processes both internally and externally. A summary of these risk assessments is provided as an attachment to this document. Each risk assessment report is also provided as attachments to this document.
2.7.1 Measures envisioned to ensure privacy for the patient

At the core of ensuring the rights of the registered is to know where data about patients is stored and what the data is and has been used for. By making copies of health data and distributing it, we increase the risk of violating the rights and freedom of the registered. We also increase the cost for our society and for the patients to ensure that the rights to control what data exists and what it is used for. The principle followed in the PraksisNett IT infrastructure is therefore to minimize the number of copies made of health data. Data about patients will therefore be stored only two places, in the health institution it was created in and in safe havens where researchers can perform advanced statistical analysis on the data.

To minimize the risk of violating the privacy of study participants we plan to implement a pseudonymisation mechanism for all patient data in the IT infrastructure. The key to re-identify the study participant will only be stored on the EHR server, together with the medical record. By storing the key together with the medical record, we ensure that participation in a medical study can be kept private and part of the patient – medical doctor relationship. Nobody else needs to know that the patient is participating in a research project. The reason for doing it this way is that participation in a research project can be as sensitive as the content of the medical record. Fear of exposing participation in a research project on a patient’s condition is one obvious reason for rejecting participation. Storing the consent form outside the health institution that recruited the patient should therefore be avoided. It should ideally be kept as part of the medical record of the patient.

Plans currently exists to store consent for participation in medical studies in national registries. The PraksisNett IT infrastructure will not make use of such registries to minimize the risks of violating the right to privacy of study participants and avoid violation of Helsinki declaration article 9.

2.7.2 New risks introduced by the PraksisNett research infrastructure IT solution

As identified in risk assessment 2: There is a risk of being identified through the aggregated data. Mitigating measures needed: A disclosure control process needs to be performed on aggregated statistics.

Unauthorised GP practice staff get access to patient information not authorised by a GP. PraksisNett must establish routines to ensure that GP Practice staff are authorised before giving GP practice staff authorisation to access patient information belonging to a specific project.

Unauthorised persons get access to the GP practice network through the remote desktop protocol, or the application communication protocol. This risk is addressed in RA5.

The data reuse server can be stolen by persons with physical access to the GP practice. This risk is addressed in RA6.

The data reuse component installed at EHR server interfering with the EHR preventing treatment of patients. This risk is addressed in RA3.

Data extraction or Emnet client providing wrong results to the GP, identifying wrong list of patients for studies or working lists. This is a new risk.

2.7.3 Measures envisioned to address new risks

In section 2.7.1, the re-identification risk from aggregated data is listed. It is an old risk, but appears in the new IT solutions. We plan to address this risk by applying functionality for
Disclosure control before visualising data to the end users or making it available through web service interfaces.

In section 2.7.1, several new risks to violation of privacy are identified. Because the first version of the functionality to authorise access to the re-identification interface of the DRC will be done by the PraksisNett staff, a possibility exists that unauthorised personnel get access to fully identified patient information belonging to a research dataset at the GP practice during the recruitment phase. Two measures can be used to avoid this risk, 1) not authorising GP practice staff for such access, 2) establishing quality assurance routines that ensure that access is granted to personnel that is approved by the responsible GP.

Another possible risk related to quality of provided data is the risk of identifying wrong patients. The cause of such an event would probably be programming errors done by the PraksisNett development team. This event will be discovered very soon as GPs and GP practice staff will notice the mismatch between the recruitment criteria of a research project and the content of the recruitment list. If such a mismatch is discovered the PraksisNett team will be notified and the error corrected.

2.7.4 Measures envisioned to ensure the right not to be discriminated

As mentioned in section 2.7.1, patients do not have the right to participate in research that can improve the treatment of future patients. Some patients view participation in research on their medical condition as a deeply meaningful and valuable action. For some patients the only hope for finding a cure or treatment is participation in research. Every GP should therefore make an assessment whether not being part of the PraksisNett research infrastructure is discriminating the patient on his list from contributing to establishing new knowledge about their medical condition.

3 References


770.


Summary of the risk assessments performed on the Snow system

Attachment to the PraksisNett the Data Protection Impact Assessment document

1 Introduction

The Snow system, which is the basis for the PraksisNett IT infrastructure has been subject to 7 risk assessments processes both internally and externally. Below follows a summary of these risk assessments.

2 Risk assessments

2.1 Risk assessment 1 – February 2008

This risk assessment is documented in the attached RA1 document. Below follows the summary from the report. The report was also the foundation for a publication focused on threats to information security of real-time disease surveillance systems[1].

Summary

The main part of this risk assessment was performed in October – November 2007. The following persons participated in the risk assessment:

Risk assessment leader: Eva Henriksen.

Project participants: Johan Gustav Bellika, Monika Johansen, Johanna Nystad, Per Atle Bakkevoll, Anders Baardsgaard (from Norwegian Health Network)

To analyse the security challenges of the Snow project, we performed a qualitative risk analysis of the information security aspects of the proposed architecture and the intended environment and use. The goal was to identify security threats to the institutions involved and to patient information confidentiality, and to find acceptable solutions to the threats. The threats were identified in two semi-structured brain storming sessions. We performed the risk analysis by going through the five main steps described in the Australian and New Zealand standard for risk management [2].

1. Context identification
2. Threat identification
3. Analysis of the identified threats with respect to likelihood and consequence
4. Calculation of risk value for each threat as the product of consequence and likelihood, illustrated in a two-dimensional matrix
5. Proposal of risk-reduction treatment for all threats with a non-acceptable risk level. This methodology corresponds very well to the ISO standard 27005 for information security risk management [3].

Main conclusions

This first high-level risk assessment of the Snow system identified no threats with an unacceptable High risk level. Only two threats have been given a Medium risk level, one of these (c1) is considered to be unacceptable. Threat c1 concerns the possibility that the information produced by the Snow service is sensitive, i.e. not anonymous “enough”. It is difficult to assess the information security risk of a system this early in its development process. Many threats can
be identified as possible unwanted incidents, but it is impossible to foresee their risk level, in particular the likelihood for it to happen. The main result at this stage is therefore that we have been able to identify threats and possible unwanted incidents, and to foresee a consequence of these. In the analysis we have focused particularly on threats with severe consequence. The argument for this is that with an increased likelihood these threats will easily get an unacceptable risk level. A tendency, based on consequence, is that all the confidentiality threats have severe consequence, while most of the availability threats have lower consequence. The integrity threats are distributed between severe and moderate consequence.

### 2.2 Risk assessment 2 – August 2010

This risk assessment is documented in the attached RA2 document. Below follows the summary from the report.

**Summary**

The purpose of the Snow service for epidemiology is early detection of disease outbreak, fast and easy notification and management of disease outbreaks. This version of Snow collects its input data from hospital laboratory tests.

In this phase of the project the Snow system is also a tool to investigate the research questions in the research project funded by Helse Nord, e.g. how the system is used.

**The risk assessment**

The main part of this risk assessment was performed in April – June 2010. The following persons participated in the risk assessment:

- Risk assessment leader: Eva Henriksen.
- Project participants: Johan Gustav Bellika, Lars Ilebrekke, Per Atle Bakkevoll, and Marit Wiklund (microbiology laboratory, UNN)

To analyse the security challenges of the Snow project, we performed a qualitative risk analysis of the information security aspects of the Snow system after it was implemented, and the intended environment and use by the microbiology lab at UNN. The goal was to identify security threats to the institutions involved and to patient information, and to find acceptable solutions to the threats. The threats were identified and analysed in six brainstorming sessions, where elements of Fault Tree Analysis (FTA) also were used in the threat identification process.

We performed the risk analysis by going through the five main steps described in the Australian and New Zealand standard for risk management [2].

1. **Context identification**
2. **Threat identification**
3. **Analysis of the identified threats with respect to likelihood and consequence**
4. **Calculation of risk value for each threat as the product of consequence and likelihood, illustrated in a two-dimensional matrix**
5. **Proposal of risk-reduction treatment for all threats with a non-acceptable risk level**

This methodology corresponds very well to the international standard ISO 27005 for information security risk management [3].

**Main conclusions**
This second risk assessment of the Snow system identified two threats with an unacceptable High risk level (q1.1 and c3). Six threats were given a Medium risk level, and five of them (a2, i2, q1.2, q1.3, and q5.1) were evaluated to be unacceptable. Among the threats with Low risk level, we focused especially on the eleven threats with severe consequence.

The risks with high level was:

Q1.1: Missing analyses from the microbiology laboratory, because analysis with new codes are not exported from laboratory system.

C3: Unauthorized persons get access to (pseudonymous) information which is also stored elsewhere, e.g. in other file systems, in other computers, on memory sticks, etc.

The risk with medium level risk was:

A2: The Snow client causes reduced performance of other systems at the user (GP) side because the web reader takes all resources on the local PC.

I2: Information in the Report DB in the coordinator server is modified by unauthorized persons through the web server.

Q1.2: Analyses from the microbiology laboratory not included, because Snow does not recognise the new analysis codes in the export files from laboratory system.

Q1.3: Analyses from the microbiology laboratory not included, because the microbiology laboratory has changed the result text (pos/neg) and Snow does not recognise the new text.

Q5.1: The coordinator server produces old information because the LabServer does not receive new extracts from the laboratory system after updates, or receives only parts of the extracted data from laboratory system.

Q4: Snow does not detect that a “new” analysis is really an earlier analysis that has been changed by the lab afterwards.

### 2.3 Risk assessment 3 – January 2012

This risk assessments is documented in the attached RA3 document. This risk assessment report focused on the Snow disease surveillance server for GP practices. Unfortunately this report is written in Norwegian. Below follows an English summary of the report.

In this risk assessment process we used the SBA SCENARIO method used by the privacy ombudsmann at the Univeristy hospital of North Norway. The process contains the following steps:

- Planning and education of participants in the scenario method
- Establishing working groups
- Establishing the agenda for the analysis
- Creative brainstorming to find possible events
- Choice of 5-10 scenariodescriptions pr group
- Description of scenario
- Uncovering the consequences of the scenario
- Identifying causes that effect the course of the scenario
- Producing a preliminary standard report

The method identified the following list of threats that were prioritised to handle by taking actions to prevent them from happening:

N5: Wrong disease surveillance data is presented by the Snow system
N4: The coordination server is compromised
N3: Patient data is deleted
N2: Bad quality on provided medical treatment of communicable diseases
N1: Patient data becomes available for unauthorised persons

20 tasks to reduce the risks was identified and performed to bring the above risks to an acceptable level. One exception was a task to prevent patient data from being deleted (N3). This task was outside the capabilities of our research group to handle.

2.4 Risk assessment  4 – July 2013

This risk assessment is documented in the attached RA4 document. This risk assessment report focused on remote management of the coordination server. Unfortunately, this report is written in Norwegian. Below follows an English summary of the report.

The Snow system coordination server needed to be moved to a secure physical location (one of the threats identified in RA3). This risk assessment focuses on a remote management solution for the coordination server. The risk assessment identified 5 risks which were all assessed to be of low likelihood. No further actions were therefore necessary to reduce the risks.

2.5 Risk assessment  5 – April 2016

This risk assessment is documented in the attached RA5 document. This risk assessment report focused on remote management of the Snow servers located in the GP practices (see also RA6). Below follows a summary of the report.

Background for risk analysis

The separation of the SNOW system components from the critical systems in the GP practices called for a more sustainable and scalable way for configuring the distributed nodes. Currently SNOW GP office nodes are distributed as standalone appliance boxes, which need to be plugged into the data network to function. Chef was selected as a framework for automating the setup and configuration of the SNOW appliance boxes.

This risk assessment analyses the threats introduced by the use of Chef and reverse SSH tunnel for managing the distributed SNOW infrastructure. Other aspects of the system have already been discussed in previously performed risk assessments and therefore are out of the scope of this document.

Conclusions

Eleven threats introduced by the use of Chef and reverse SSH tunnel for managing the SNOW infrastructure were identified. All of them were characterized as acceptable, given the currently implemented security mechanisms.

2.6 Risk assessment  6 – May 2016

This risk assessment is documented in the attached RA6 document. This risk assessment report focused on Snow appliance boxes that are installed inside the GP practices. Unfortunately, this report is written in Norwegian. Below follows an English summary of the report.

Background for the risk assessment

During spring 2015 the Snow project started evaluating the possibility of using dedicated
hardware for the server that was developed by the Snow project, which was previously run on
the EHR server of the general practice practices. The purpose of using dedicated hardware
was to minimize the risk of affecting the electronic health record systems, which was possible
when computer hardware was shared between the electronic health record system and the
Snow system (see section 2.8.3). This risk assessment tries to clarify whether new non
acceptable threats appear as a consequence of using dedicated hardware for the Snow
software within the GP practices.

Main conclusions

The use of dedicated hardware for services developed by the Snow project minimises the risk
of disturbing the operations of the GP practices and resolve the risk identified in risk
assessment 3 (see section 2.8.3). At the same time a system for remote management of the
server is introduced which allows deployment of the servers while the services are being
developed (see section 2.8.5). Unauthorised access to EHR data and to Snow services are the
main threats. The security measures that has been implemented reduced the risks to
acceptable levels.

2.7 Risk assessment 7 – June 2016

This risk assessment was performed by Hemit, as part of installing a Snow server for the
Snow disease surveillance service in Helse Midt. Unfortunately, this report is written in
Norwegian. Below follows an English translation of the summary of the report.

This risk assessment was performed with the information available on the time of the
analysis. The assessment was performed by resources from Hemit and from the Norwegian
centre for e-health research. The main conclusion from the assessment is that there is low risk
involved in installing and operating a Snow-server on St. Olavs Hospital.

Some risk is involved in unauthorised access to pseudonymised data and unintentional access
to the Snow server in the secure zone. Existing measures to avoid these threats is assessed to
be sufficient. However, 5 new countermeasures can contribute to reduce the risk even further.
These measures are securing the server and new routines at the microbiology lab. These are
described in relation to each threat.

3 References

1. Henriksen E, Johansen MA, Baardsgaard A, Bellika JG. Threats to Information Security
   5.

2. Standards Australia, editor. Risk management. Strathfield: Standards Association of

3. ISO/IEC 27005 risk management standard [Internet]. [cited 2017 Jun 23]. Available from:
Risk assessment report

The SNOW project

Version 1.00
07.02.2008

Eva Henriksen, Johan Gustav Bellika,
Anders Baardsgaard (NHN), Johanna Nystad, Per Atle Bakkevoll, Monika Johansen

Norwegian Centre for Telemedicine
Summary

The project
The purpose of the Snow service for epidemiology is early detection of disease outbreak, fast and easy notification and management of disease outbreaks.

The risk assessment
The main part of this risk assessment was performed in October – November 2007. The following persons participated in the risk assessment:
- Risk assessment leader: Eva Henriksen.
- Project participants: Johan Gustav Bellika, Monika Johansen, Johanna Nystad, Per Atle Bakkevoll, Anders Baardsgaard (from NHN)

To analyse the security challenges of the Snow project, we performed a qualitative risk analysis of the information security aspects of the proposed architecture and the intended environment and use. The goal was to identify security threats to the institutions involved and to patient information confidentiality, and to find acceptable solutions to the threats. The threats were identified in two semi-structured brain storming sessions.

We performed the risk analysis by going through the five main steps described in the Australian and New Zealand standard for risk management [3].
1. Context identification
2. Threat identification
3. Analysis of the identified threats with respect to likelihood and consequence
4. Calculation of risk value for each threat as the product of consequence and likelihood, illustrated in a two-dimensional matrix
5. Proposal of risk-reduction treatment for all threats with a non-acceptable risk level

This methodology corresponds very well to the upcoming ISO standard 27005 for information security risk management [4].

Main conclusions
This first high level risk assessment of the Snow system identified no threats with an unacceptable High risk level. Only two threats have been given a Medium risk level, one of these (c1) is considered to be unacceptable. Threat c1 concerns the possibility that the information produced by the Snow service is sensitive, i.e. not anonymous “enough”.

It is difficult to assess the information security risk of a system this early in its development process. Many threats can be identified as possible unwanted incidents, but it is impossible to foresee their risk level, in particular the likelihood for it to happen. The main result at this stage is therefore that we have been able to identify threats and possible unwanted incidents, and to foresee a consequence of these.

In the analysis we have focused particularly on threats with severe consequence. The argument for this is that with an increased likelihood these threats will easily get an unacceptable risk level. A tendency, based on consequence, is that all the confidentiality threats have severe consequence, while most of the availability threats have lower consequence. The integrity threats are distributed between severe and moderate consequence.
# TABLE OF CONTENT

**SUMMARY** ............................................................................................................................................................... 2  
  The project ........................................................................................................................................................ 2  
  The risk assessment........................................................................................................................................... 2  
  Main conclusions .............................................................................................................................................. 2  

## 1 INTRODUCTION .......................................................................................................................................... 4

## 2 CONTEXT IDENTIFICATION ................................................................................................................... 5
  2.1 DESCRIPTION OF SYSTEM AND SERVICES ................................................................................................. 5  
  2.2 SECURITY REQUIREMENTS ....................................................................................................................... 9  
    2.2.1 Legal baseline .................................................................................................................................... 9  
    2.2.2 Requirements to the Snow service ................................................................................................... 10  
  2.3 DEFINITION OF LIKELIHOOD, CONSEQUENCE AND RISK LEVELS ............................................................ 11  
    2.3.1 Likelihood and consequence levels.................................................................................................. 11  
    2.3.2 Acceptance criteria .......................................................................................................................... 12  
    2.3.3 Risk levels ......................................................................................................................................... 13  

## 3 THREAT IDENTIFICATION AND ANALYSIS OF RISK................................................................... 14
  3.1 THREATS WITH HIGH RISK LEVEL .......................................................................................................... 15  
  3.2 THREATS WITH MEDIUM RISK LEVEL .................................................................................................... 15  
  3.3 THREATS WITH LOW RISK LEVEL........................................................................................................... 16  

## 4 CONCLUSIONS AND RECOMMENDATIONS..................................................................................... 18
  4.1 RECOMMENDED RISK TREATMENT ........................................................................................................ 18  
    4.1.1 Treatment of threats with Medium risk............................................................................................ 19  
    4.1.2 Treatment of severe threats with Low risk.......................................................................................2 0  
  4.2 FURTHER INVESTIGATIONS NEEDED ...................................................................................................... 22  
  4.3 CONCLUSIONS ........................................................................................................................................ 23  

**REFERENCES** ....................................................................................................................................................... 24

**ABBREVIATIONS**................................................................................................................................................. 25

**ANNEX A**  THREAT TABLE .......................................................................................................................... 26

**ANNEX B**  PLAN FOR IMPLEMENTATION OF SECURITY MEASURES ................................................................. 35

**ANNEX C**  DESIGN ISSUES RELATED TO PRIVACY AND SECURITY......................................................... 39
  C.1 PRESERVE PRIVACY OF DATA FROM A SMALL DATA SET .................................................................... 39
1 Introduction

Risk analysis of information security is a basic requirement of ISO 27002 (formerly ISO 17799), internationally recognized as “the generic information security standard” [1]. Risk analysis is also required by national legislation as a vital part of an information security management system for any organisation. Risk analysis is performed with respect to the main information security aspects Confidentiality, Integrity and Availability. The risk acceptance criteria are defined by the information security policies of the affected organisation.

There are many methods and guidelines for how to perform risk analysis, but all of them include the central tasks of:

- identifying the threats or possible unwanted incidents
- analysing the impacts and probabilities of these threats
- evaluate risks with respect to the acceptance criteria

Our experience is based on the EU-funded research project CORAS from the fifth framework programme (FP5) of Information Society Technology (IST) [2] where a methodology for risk analysis was developed and tested on e-health systems. The methodology was based on the Australian and New Zealand standard for risk management (AS/NZS 4360/1999) [3], which clearly sets out the risk analysis process in five main steps:

1. Context identification; a description of the subject for analysis, i.e. the analysed system and its environment.
2. Threat identification; identify what could possibly happen.
3. Impact and probability analysis; a consideration of the consequences of the threats and the likelihood that these consequences may occur.
4. Risk evaluation; relating the resulting risk level with risk acceptance criteria.
5. Risk treatment; identification and assessment of treatment options.

Lately, the upcoming ISO standard 27005 for Risk Management in Information Security Management Systems [4] are built around a very similar approach.
2 Context identification

The Snow system is a peer-to-peer system that can be used for exchange of any kind of information between health institutions. In this risk assessment we only consider the Snow system as a decentralised disease surveillance system. The Snow system is in this context used to extract and distribute data about occurrences of communicable diseases from electronic health records systems (EHRs) within general practitioners’ offices. We also want to exchange text-based messages using the Multi User Chat (MUC) service available in the Instant Messaging service which the Snow system is built on top of.

The subsystems and interfaces of the Snow service are illustrated in figures 1 and 2 below. The following subsystems have been subject for analysis in this risk assessment:

The client side:
- Text conferencing and Instant Messaging (IM) tool.
- The Snow Agent System Client is integrated with the IM client tool.

Together, these tools are used by the end users to receive textual information, and to initiate agent missions to collect, assemble and visualize disease surveillance data.

The server side components:
- The Mission Controller component (MC) which controls and manages agent missions on behalf of a client or Agent, by creating, monitoring, and terminating agent missions.
- The Agent Daemon component (AgD) which initiates the agent processes on the Snow Agent System servers, based on a Mission Specification from the requesting MC.
- The Agent application (disease surveillance specific) which performs local information retrieval and processing according to the mission specification.
- The Poller component (installed in the most secure zone) which is used to poll a server in the health network (less secure zone) for messages. The Poller is a technical solution to ensure that information is not sent from a less secure zone into a more secure zone.
- Post office (PO) component (installed in the health network) which is used to store and route messages on behalf of the servers located in the more secure zones. The PO could also have additional functionality like merging data for a region (processing of single results into aggregates).

Together the client and the server side components form the Snow Agent system.

2.1 Description of system and services

The system consists of clients used by end users and server(s) located in the health network, called post offices, in addition to the Snow Agent System (SAS) servers installed on the GP office’s EHR server machines. The servers work together to provide the disease surveillance service. The servers are more or less identical:

- **General server features:** All servers provides the following features:
  - Cache of latest results
  - Snow institutional membership list
  - User database
  - Data needed to map geographical areas to data provider lists
  - Geographical data to produce surveillance maps
  - Demographic data from the local population used to produce disease statistics
- **Local level**: At this level data is extracted from the EHR systems. This is also where most of the targeted end users of the service are located. The end users use clients to request and view information provided by the set of servers. The Snow Agent System (SAS) server in each GP office is normally located on the same machine as the EHR server, but can also be located on a dedicated server. Specialised features:
  - Access patient information in the local EHR server

- **OPTIONAL: Regional (intermediate) level**: Dependent on the size of the surveillance network, a separate level for merging regional data may be needed. The Snow PO (Post Office) servers are used for this purpose. These servers merge data from all GP office Snow servers that is serviced by the post office. If an intermediate level is needed, data is forwarded to the top level which is described below. Specialised features:
  - Post office functionality (store and route messages)
  - Intermediate data merging

- **Top level**: Independent of surveillance network size there always exist an entity that merges all the surveillance data together and produce the final end result that is provided to the end user(s). This entity is called the “main agent”. The main agent is always the first process instantiated within a mission. Based on the specification of the epidemiological query the data provider list is constructed and disease statistics are requested from the local level by doing data extraction from the local EHR systems. Specialised features:
  - EHR data extraction request construction
  - Final data merging and end result production

Figure 1 shows the details of the Snow server at the **local level**. The Agent Daemon acts as a guardian for the local data, processor and storage. It constitutes the Ministry of Home affairs, if compared to a political system. This component is the entity responsible for initiating the processes (named Snow Agent in Figure 1) that extracts data from the EHR system. A Snow Agent process is created from a repository of trusted software that is stored locally and created during install and upgrade of the Snow server. Figure 1 also shows the local data cache that is used to provide fast response when multiple requests ask for the same data. The Mission Controller (MC) represents the Ministry of Foreign Affairs in our analogue to political systems. Its responsibility is to control computations performed on remote servers. It provides mission control service on behalf of local users and agents requested from remote servers. The MC always knows the whereabouts of agents belonging to the local users, but running on other sites. It may also provide migration or mission control service on request from locally running agents.
In Figure 1 the Snow Agent is shown as accessing information in the EHR system or the EHR database. Figure 2 shows how and on what basis the agent is constructed. Normally the user sends a request to a Mission Controller (MC) in form of an XML message containing a “Mission specification” labelled “Request” in figure 2. The Mission Controller forwards this request to one or more remote agent daemons, depending of the type of service requested. If the Agent Daemon (AgD) accepts the request, a process (agent) is constructed from the local software repository shown in figure 1. After instantiation the agent performs the requested action, in this case to extract disease statistics from the local EHR system. To provide statistics, all local data are made anonymous and then transferred out of the local system for further processing as explained above. Both agents and clients can request mission control service from MC. If the word “client” is replaced by “Main Agent”, figure 2 shows how the main agent requests data from the EHRs which have data that is requested in the “mission specification” for the disease surveillance service.
Figure 3: Architecture of the Snow system when Firewalls are used

Figure 3 shows the architecture of the system when firewalls are used to protect the GP office local area network for someone initiating a TCP connection into the software services inside the GP office. The “C” represents clients, The “S” represents Snow agent servers and the “PO” represents the “Post office” Snow agent server that enables communication between the participating institutions. Between the servers S1 and PO, and S2 and PO, we use the Poller and post office (PO) components mentioned above. The PO may run the “Main agent” described above and/or the intermediate regional PO process, if many servers are involved.

Figure 4: UML sequence diagram for a disease statistics extraction agent mission [5]
Figure 4 shows the sequence of actions performed by the involved actors to produce disease statistics. Time starts at the top and moves downwards, the grey boxes represents different machines where the rightmost represents the Snow agent server located on the same server as the EHR server in the GP office. The white vertical lines represent active processes. The diagram shows that “Main EPI Ag”, or the “Main agent”, is the first process instantiated. The Main agent requests processing of the “EHR EPI Ag”, i.e. the disease statistics extraction agent, which transmits the statistics to the Main agent for merging of data into the final result. The diagram does not show that many EHR EPI Ag processes may work simultaneously.

More information about the system and services are given in published papers [5] and [6] and in reports under www.telemed.no/opensource/snow.

2.2 Security requirements

Privacy is always an issue when patient data is involved. Protection of patient privacy is therefore an important issue to address for a disease surveillance system [6].

2.2.1 Legal baseline

Privacy requirements related to communication of sensitive patient-identifiable information establish the baseline for the information security needs. Confidentiality requirements originate from the professional secrecy and non-disclosure agreement imposed to all healthcare workers. Requirements to electronic communication of patient information come from national legislation in European countries, which are also based on EU’s regulation on processing of personal data (Directive 95/46/EC) from 1995 [7]. At the lowest level these requirements become apparent through the security policies of the affected organisation.

According to Norwegian legislation, all health-related information concerning an identifiable person is considered sensitive information (Personal Data Act (Personopplysningsloven) §2) [8]. No one else than those who have a treatment relation to the person, should be able to access this person’s health information, unless the patient has given his or her consent.

Norwegian legislation requires risk assessment as part of an information security management system for any organisation. The legislation also defines information security to include the following aspects: Confidentiality, Integrity, Quality, and Availability [8, 9]. The risk assessment is performed with respect to these information security aspects.

Personal identifiable information (PII) is any information that can identify a physical/natural person. The definition of personal information in the EU Directive [7] reads: “Personal data shall mean any information relating to an identified or identifiable natural person (“data subject”); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity”.

The “Article 29 group” is a “working party on the protection of individuals with regard to the processing of personal data”.1 It has been formed with the regard to the EU Directive [7], in particular with regard to Article 29 and paragraph 1(b) of Article 30. (Hence the chosen short-name.) – In [11] the “Article 29 group” analyses further the concept of Personal Data. They state that ”a person may be identified directly by name or indirectly by a telephone number, a car registration number, a social security number, a passport number or by a combination of significant criteria which allows him to be recognized by narrowing down the group to which

---

he belongs (age, occupation, place of residence, etc.)”. This indicates that it also depends on
the context of the particular situation which identifiers are sufficient to achieve identification.

On the other hand, if the information is anonymous it is not defined as personal identifiable
information and not subject to the legislation given by the EU Directive [7] or the Norwegian
Personal Data Act [8].

The Article 29 group defines anonymous data as any information relating to a natural person
where the person can not be identified, neither by the data administrator nor by any other
person, neither directly or indirectly. They state that a hypothetical possibility to single out the
individual is not enough to consider the person as “identifiable”: If, taking into account “all
the means likely reasonably to be used by the controller or any other person”, that possibility
does not exist or is negligible, the person should not be considered as “identifiable”, and the
information would not be considered as “personal data”.

One example: The description “gender: Male; age: 50-59; occupation: Bus driver” is
anonymous if we consider the whole population of Norway, or even Oslo. But if we consider
the population of a small municipality of less than 1000 inhabitants, this could point directly
to one specific person.

If the intention is to keep the information anonymous, the Article 29 group states: If a
criterion appears to lead to identification in a given category of persons, however large (i.e.
only one doctor operates in a town of 6000 inhabitants), this “discriminating” criterion
should be dropped altogether or other criteria be added to “dilute” the results on a given
person.

The Article 29 group concludes that the assessment of whether the information can be
considered as anonymous, or the data identifies an individual, depends on the circumstances.
A case-by-case analysis is therefore needed. Further, they state that: This is particularly
relevant in the case of statistical information, where despite the fact that the information may
be presented as aggregated data, the original sample is not sufficiently large and other pieces
of information may enable the identification of individuals.

2.2.2 Requirements to the Snow service

The information handled by the Snow system is health-related information. Consequently, if
the information is person identifiable (i.e. not anonymous) it will also be sensitive.

A core privacy principle in the design of the Snow system is to keep the sensitive person
identifiable health data locally at each GP office and not transfer it to a central site for
processing [5]. Information processing can be performed locally at the GP office, and only
anonymous information should be communicated by Snow.

The question is whether we really manage to keep it anonymous. What about demographical
and geographical information? One thing is to remove information that can identify a person
directly or indirectly, such as name, telephone number, social security number, passport
number, etc. But a person may also be recognized by narrowing down the group to which he
belongs (age, place of residence, occupation, etc.). For Snow the “narrowing down” is
especially related to the size of the population in the selected geographical area (e.g. covering
one postal code zone) and to the infrequency of the diagnosis (prevalence).

There are several worries that could be expressed by the GPs who are asked to be included in
the Snow service [5]:

---

2 Refer to the bus driver example in section 2.2.1
- Confidentiality and privacy: Is the transferred information really anonymous? Could it cause a deliberate or unintentional dump of patient data (from EHR) on the Internet?
- Availability of the local EHR: Can the new software interfere with the EHR system? Can the Snow agents contain malicious software (i.e. are they Trojan Horses)? Has Snow the capacity to bring down the EHR system in a GP’s office due to programming errors? Could it take all computing resources away from the GP’s local systems?
- Quality and representativeness: How widespread is the service? – The quality of the information is dependant on the correctness of the retrieved data and the coverage of the Snow service among the GPs.

2.3 Definition of likelihood, consequence and risk levels

We have chosen to use qualitative values for likelihood, consequence and risk levels.

2.3.1 Likelihood and consequence levels

We decided to use four levels for identification of likelihood and four levels for identification of consequence. The levels are defined in table 1 and table 2.

The likelihood levels can be described as frequency values or with respect to how easy it is for a person to exploit a threat. For some threats it is easier to think of the likelihood in the form of frequency or a probability value. This may often be the case for threats related to availability, e.g. caused by problems in sw or hw. For other threats it is easier to think of likelihood when related to ease of misuse or mistake, or to motivation for performing a malicious action. – For each threat or unwanted incident we choose the most appropriate column or the column that is easiest to use in order to estimate the likelihood for the threat.

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Frequency</th>
<th>Ease of misuse and motivation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very high</td>
<td>Very often, occurs more often than every 10th connection, i.e. more frequently than 10 % of the time/cases.</td>
<td>Can be done without any knowledge about the system; or without any additional equipment being used; or it can be performed by wrong or careless usage.</td>
</tr>
<tr>
<td>High</td>
<td>Quite often. Occurs between 1 % and 10 % of the time/cases.</td>
<td>Can be done with minor knowledge about the system; or without any additional equipment being used; or it can be performed by wrong or careless usage.</td>
</tr>
<tr>
<td>Moderate</td>
<td>May happen. Occurs between 0.1 % and 1 % of the time/cases.</td>
<td>Normal knowledge about the system is sufficient; or normally available equipment can be used; or it can be performed deliberately.</td>
</tr>
<tr>
<td>Low</td>
<td>Rare. Occurs less than 0.1 % of the time/cases.</td>
<td>Detailed knowledge about the system is needed; or special equipment is needed; or it can only be performed deliberately and by help of internal personnel.</td>
</tr>
</tbody>
</table>

The consequence levels are described in terms of consequences for the patient (user) and consequences for the service or the service provider. In this case the service provider could be both the GP office (seen from the patient’s viewpoint) and/or the project owner and the Snow service (seen from the GP’s viewpoint).
For each threat or unwanted incident we choose the most appropriate description to estimate the consequence level for the threat.

### Table 2: Definition of consequence levels

<table>
<thead>
<tr>
<th>Consequence:</th>
<th>For the patient: No impact on health; or negligible economic loss which can be restored; or small reduction of reputation in the short run.</th>
<th>For the service provider: No violation of law; or negligible economic loss which can be restored; or small reduction of reputation in the short run.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Small</td>
<td>For the patient: No direct impact on health or a minor temporary impact; or economic loss which can be restored; or small reduction of reputation caused by revealing of less serious information (e.g. blood pressure level).</td>
<td>For the service provider: Offence, less serious violation of law which results in a warning or a command; or economic loss which can be restored; or reduction of reputation that may influence trust and respect.</td>
</tr>
<tr>
<td>Moderate</td>
<td>For the patient: Reduced health; or a large economic loss which cannot be restored; or serious loss of reputation caused by revealing of sensitive and offending information.</td>
<td>For the service provider: Violation of law which results in minor penalty or fine; or a large economic loss which cannot be restored; or serious loss of reputation that will influence trust and respect for a long time.</td>
</tr>
<tr>
<td>Severe</td>
<td>For the patient: Death or permanent reduction of health; or considerable economic loss which cannot be restored; or serious loss of reputation which permanently influences life, health, and economy.</td>
<td>For the service provider: Serious violation of law which results in penalty or fine; or considerable economic loss which cannot be restored; or serious loss of reputation which is devastating for trust and respect.</td>
</tr>
<tr>
<td>Catastrophic</td>
<td>For the patient: No impact on health; or negligible economic loss which can be restored; or small reduction of reputation in the short run.</td>
<td>For the service provider: No violation of law; or negligible economic loss which can be restored; or small reduction of reputation in the short run.</td>
</tr>
</tbody>
</table>

### 2.3.2 Acceptance criteria

We use accept criteria to define the acceptable risk level for the service. We cannot expect to achieve a risk level equal to zero. Thus we have to define which level of risk we consider as acceptable for the service we are analysing. The accept criteria should be based on the security requirements for the service.

The Norwegian Health Personnel Act (Helsepersonelloven) states in chapter 5 the obligation to maintain secrecy with respect to health information a person has been acquainted with in his or her duty as health personnel [10].

The following acceptance criteria have been proposed for the Snow service:

It is not acceptable that:

1. (C) – the likelihood is higher than low that unauthorised persons (i.e. anyone else than the patient, and those who have a treatment relation to the patient) get access to the patient’s personal health data (i.e. to sensitive data). This is regardless of why, where, and how it happens. *(This means that in order to obtain unauthorised access to such data, detailed knowledge is needed about the technical system, or special equipment is needed, or it can only be performed by help of internal personnel.)*

---

3 These are the same four consequence levels as used by Helse Nord in their template for risk assessments.
4 The letter in parenthesis refers to the security aspects confidentiality (C), integrity (I), availability (A)
2. (A) – the likelihood is higher than **low** that the Snow service causes the local EHR system to be down for a period of time. *(This corresponds to up to 2.4 minutes of a 40 hours work week, or that it happens more infrequent than once for every 1000 Snow accesses.)*

3. (A) – the likelihood is higher than **low** that the Snow service causes data in the local EHR system to be destroyed. *(I.e. that it happens more infrequent than once for every 1000 accesses to the Snow service.)*

4. (A) – the likelihood is higher than **moderate** that the Snow service is unavailable for a period of time. *(This corresponds to up to 24 minutes of a 40 hours work week, or that it happens not more than once for every 100 Snow accesses.)*

5. (I) – the likelihood is higher than **low** that the Snow service causes information in the local EHR system to be modified. *(I.e. that it happens more infrequent than once for every 1000 accesses to the Snow service.)*

6. (I) – the likelihood is higher than **low** that information in the Snow system (request, results) are being modified. *(I.e. more infrequent than once for every 1000 accesses to the Snow service.)*

### 2.3.3 Risk levels

We have decided to use three distinct levels for risk: **Low, Medium, and High**. Our risk level definitions are presented in table 3.

The risk value for each threat is calculated as the product of consequence and likelihood values, illustrated in a two-dimensional matrix (figure 5). The shading of the matrix visualizes the different risk levels. Based on the acceptance criteria, the risk level **High** is decided to be unacceptable. Any threat obtaining this risk level must be treated in order to have its risk reduced to an acceptable level.

#### Table 3: Definition of risk levels

<table>
<thead>
<tr>
<th>Risk level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>Acceptable risk. The service can be used with the identified threats, but the threats must be observed to discover changes that could increase the risk level.</td>
</tr>
<tr>
<td>Medium</td>
<td>The risk can be acceptable for this service, but for each threat the development of the risk must be monitored on a regular basis, with a following consideration whether necessary measures have to be implemented.</td>
</tr>
<tr>
<td>High</td>
<td>Not acceptable risk. Can not start using the service before risk reducing treatment has been implemented.</td>
</tr>
</tbody>
</table>

#### Figure 5: Risk matrix showing the defined risk levels

<table>
<thead>
<tr>
<th>Consequence:</th>
<th>Small</th>
<th>Moderate</th>
<th>Severe</th>
<th>Catastrophic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Likelihood:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
</tr>
<tr>
<td>Moderate</td>
<td>Low</td>
<td>Medium</td>
<td>Medium</td>
<td>High</td>
</tr>
<tr>
<td>High</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Very high</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
<td>High</td>
</tr>
</tbody>
</table>
3 Threat identification and analysis of risk

Approximately 30 threats and unwanted incidents have been identified. The threats are listed in the threat table in Annex A. For each possible threat we wanted to evaluate its impact or consequence and the likelihood that it would occur. Threats were given qualitative values for consequence and likelihood, according to definitions in tables 1 and 2.

Many of the threats have, however, been difficult to analyse with respect to consequence and in particular with respect to likelihood. It is problematic in the design phase to imagine the likelihood for possible unwanted incidents to happen in a system that has not yet been fully implemented. However, we have more than ten years of research activity on this concept.

At this early stage we do not know what the user interface will look like. Typically, we have not been able to analyse the likelihood for threats related to software development (software errors/bugs, software functionality, wrong usage), and it is also difficult to evaluate quality threats resulting from limited use and coverage (too few users). It is much easier to foresee consequences of these threats and possible unwanted incidents.

The risk value for each threat\(^5\) is calculated as the product of consequence and likelihood values. The unique ID of the threat is written into the corresponding cell of the matrix, as shown in figure 6.

**Figure 6: Risk matrix for the Snow service**

<table>
<thead>
<tr>
<th>Likelihood:</th>
<th>Small</th>
<th>Moderate</th>
<th>Severe</th>
<th>Catastrophic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>a7a</td>
<td>a2, a3a, a4, a5, a6b, a7b, i2, i3a, i3b</td>
<td>g2, c2a, c2b, c3, c4, c5, a1a, a1b, i1a, i1b</td>
<td></td>
</tr>
<tr>
<td>Moderate</td>
<td>a6a</td>
<td>c1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>High</td>
<td>a3b</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Very high</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The placing of the identified threats in the risk matrix shows a particular tendency: Most of the threats have been analysed to have a Low risk level. It is mainly the likelihood for these unwanted incidents that has been evaluated to be Low. First of all this is related to the problems, mentioned above, of analysing a system which is in its early design phase.

Ten of the threats have, however, been analysed to have Severe consequence. If the likelihood for these threats increases, their risk level will soon be unacceptably high. This is for instance the case for all the threats related to confidentiality (c1-c5). For these threats we can argue that the low likelihood is based on two important design assumptions:

\(^5\) The following threats from the table in Annex A have not been given a risk value and are therefore not included in the matrix: g1, a8a, a8b, a9, q1a, q1b, q2, q3
- The information that is retrieved from the EHR is (meant to be) anonymous
- End-to-end encryption is imposed between Snow nodes.

The matrix also shows that while all the confidentiality threats are analysed to have Severe consequence, most of the threats to availability (and integrity) are analysed to have a lower consequence. A reason for this is that while confidentiality breaches are violation of law, the consequences of availability breaches in this case are more related to the trust and reputation of the Snow service. (This could of course in some cases be devastating for Snow.) It is also a tendency that threats to availability and integrity of the local EHR system are considered more serious than similar threats to availability and integrity of the Snow system.

Some of the identified threats are discussed in more detail in the following subsections.

### 3.1 Threats with High risk level

In this analysis none of the threats have got an unacceptable high risk level.

### 3.2 Threats with Medium risk level

Only two threats have got a medium risk level. Even if these in principle could be acceptable risks, each of them should be investigated separately to see if they can cause additional problems. In this case the conclusion is that one of them (c1) is unacceptable, while the other (a3b) can be accepted.

**c1 – Sensitive (i.e. person identifiable) information is extracted from the EHR by the agents, and communicated in the Snow system.**

The likelihood for this threat is uncertain, but is analysed to be higher than low. According to acceptance criterion 1 in section 2.3.2 this threat is therefore unacceptable: “It is not acceptable that the likelihood is higher than low for unauthorised persons to get access to sensitive data.” – It is difficult to suggest a likelihood for this to happen. Originally, we have said that this must be further investigated. But we predict that if this is not especially handled by the functionality of the system, the likelihood will be more than Low (i.e. at least Moderate).

The consequence is analysed to be severe for the system/service. Revealing this kind of sensitive information is a violation of law which could result in penalty or fine, and it would cause a serious loss of reputation that will influence trust and respect for the Snow system/service for a long time (maybe forever).

The legal baseline and definitions of person identifiable information (PII) and anonymous information is discussed in section 2.2.1 above.

When considering whether the information is anonymous, one must also take into account the possibility of design and programming errors in the development of this functionality of the Snow service.

**a3b – Increased load on the local systems at the GP office, and correspondingly decreased responsiveness, because of features in the Snow system.**

Examples of such features in the Snow system could be that too many missions (requests) and corresponding agents are executing simultaneously. It could, for instance, happen during outbreaks that many GPs issue similar requests at the same time. Load problems could be

---

6 Even if the consequence is not Severe, but only Moderate, the Risk level will still be Medium.
caused by missing limitations/restrictions imposed in the system, or by errors/bugs or wrong configuration.

This threat is analysed to have moderate consequence, or less. It depends on how often and how long they experience problems with decreased responsiveness. The result of this threat is mainly annoyance for the user (GP) and reduced reputation for the Snow system. On the other hand, we have indicated a high likelihood for this threat, merely to point at the importance of taking care of the load problem during design and implementation.

If the increased load does not cause the local EHR system to be completely down for a period of time, this is considered an acceptable risk (acceptance criterion 2 in section 2.3.2).

In connection to this threat, we refer to paper [6] which documents the scalability of the Snow system and concludes that the responsiveness of the Snow system is minimally affected when the number of Snow participants grows.

### 3.3 Threats with Low risk level

The remaining 20 threats have a low risk level. These are therefore acceptable risks, but one should occasionally keep an eye on them to see if they can cause new problems. Some of the risks could for instance change due to modifications of the service.

It is particularly important to observe the ten low-risk-threats which have been analysed to have severe consequence. If the likelihood for these threats increases, their risk level will soon be unacceptably high. This could happen if the communication is done without encryption and the information transferred is not anonymous. The low risk threats with severe consequence are therefore discussed separately here.7

**g2 – False or bogus software modules can be installed on the Snow servers or in the GP’s local systems.**

Such false modules must be considered malicious software (malware). They can do all sorts of harm to the confidentiality, integrity, and availability of the information and the service, and lead to a lot of other threats. For example, a fake/bogus client could send a request to a corresponding fake/bogus agent which extracts patient id information from the EHR.

If this happens it will be devastating for the trust and reputation of the Snow system/service. The likelihood, however, has been set to low because this is foreseen to be taken care of in the development of the system, by several means. For instance, the access rights to the EHR database must be limited with respect to which information that can be extracted. The malicious software must then, in addition, be able to modify or overrule these access rights.

**c2a – Sensitive information from the GP’s EHR is revealed to unauthorised persons by false or bogus agents that are able to extract sensitive information from the local EHR.**

This threat is directly related to threat g2 above. If it is not possible to introduce such fake/bogus software modules into the Snow system, this threat disappears more or less.

**c2b – Sensitive information from the GP’s EHR is revealed to unauthorised persons because errors/bugs in the Snow software makes it possible to extract sensitive information from the local EHR.**

The likelihood for this to happen is probably lower than the likelihood for threat c2a above. The Snow system’s access rights to the EHR database will be limited, and a programming

---

7 Low-risk-threats with consequence analysed to be lower than severe, are not discussed here.
error would not be able to violate these rights. – On the other hand, there could also be an error in the setting (configuration) of the access rights to the EHR database.

**c3 – Sensitive information is exposed during transfer because of wiretapping, unauthorised persons “listening in” to the communication.**

The likelihood for this risk is foreseen to be (very) low because end-to-end encryption will be imposed on the communication. And this adds to the fact that the information extracted and transferred is intended to be anonymous and thus not sensitive. (See the discussion of threat c1 in section 3.2 above.)

**c4 – The GP intentionally performs a copy-paste operation from the EHR into a message which is submitted to the JID for a receiver**

It can be discussed whether this threat should be analysed in our context at all, because it is heavily connected to the GP’s own ethics and law obedience. If the GP wants to distribute such information he will have several means to do so, e.g. e-mail. The only reason to include this as a possible threat is that the Snow system gives the doctors a new and easy-to-use tool for communication with colleagues.

It is very difficult to give any likelihood for this threat, but the consequence if this happens is considered to be severe.

**c5 – Unintentional delivery of information from GP, caused by an unintentional copy-paste, or by sending a message to a wrong receiver address (JID)**

Also for this threat it is very difficult to anticipate a likelihood. An incident like this is related to the possibility of wrong use of the system, and thus to usability aspects of the user interface of the Snow service. – Is it too easy to place sensitive information into a message? Is it too easy to send a message to a wrong JID? For instance, if the “disease prevention doctor” wants to send (multicast) a message about a possible epidemiological outbreak to all GPs in his area, is it then possible that he, by incidence, also includes the JID to another receiver?

**a1a, a1b – The Snow system crashes the local EHR server, which results in either disk crash with destroyed data or the EHR system being unavailable for a period of time.**

These incidents could be caused by malicious DoS-attack utilizing weaknesses in the Snow system, or by other errors/bugs in Snow. In the case of disk crash, we must assume that the GP offices have established their own information security management system which also includes verified routines for backup and restore of data.

These incidents are of course serious for the GP office that loses their EHR system for a while, but the consequence is even worse for the trust and reputation of the Snow service.

**i1a, i1b – The Snow system causes modification of data/information and relations in the local EHR system, which results in wrong patient treatment.**

This could be caused by false/fake/bogus software modules doing this type of harm maliciously (see threat g2 above), or it could be caused by errors/bugs in the Snow system. But the Snow modules do not need write access to the EHR database, so either the malicious software must also modify the access rights to the database, or the configuration of the access rights must be wrong. – The motivation for someone to intentionally modify information in the EHR is considered to be very small, and the likelihood that someone will use Snow to do that is therefore considered being minimal.
4 Conclusions and recommendations

4.1 Recommended risk treatment

There are basically four different approaches to handle a risk [3, 4]:

1. **Accept** the risk, in accordance with the organisation’s security policy. This approach is usually applied for the risks with an acceptable risk level. *It is worth remembering that accepting the risk does not mean accepting the unwanted incident indicated by the threat.*

2. **Reduce** the risk to an acceptable level. Since the risk is a product of likelihood and consequence, this means to reduce the likelihood, the consequence, or both. It is often difficult to reduce the consequence of a threat, so the focus should first of all be on reduction of the likelihood.

3. **Avoid** the risk, i.e. try not to be exposed to the risk, not do the things that could lead to the risk. (In our case this could mean not installing the Snow service.)

4. **Transfer** the risk to a third party (e.g. an insurance company)

In this analysis we will mainly stick to strategies 1 and 2 above and recommend security measures that can reduce risks to an acceptable level. Risk reduction should be subject to a cost/benefit analysis, and if cost effective, risks should be reduced based on the ALARP principle (As Low As Reasonable Possible).

There are also examples of using *risk avoidance* (3) as a strategy, and *risk transfer* (4) could possibly be considered for threats to the local EHR systems.

The table in Annex B lists the threats with risk level Medium (from section 3.2) and the threats with Severe consequence (from section 3.3), together with security measures proposed for treatment of these threats. Treatments of each of these threats are discussed in more detail in sub-sections 4.1.1 and 4.1.2.

Some of the other threats with Low risk level will also benefit from treatment proposed to threats with higher risk. Table 4 summarizes the proposed treatments for risk reduction, and lists all the threats that would have their risk reduced by implementing these treatments. Different treatment options are grouped under a few main headings, indicating the need for routines to be defined, design decisions and configuration, encryption, quality assurance, and user training. But even if treatment options are grouped in this way, they are also depending on each other, and risk treatments for a certain threat will therefore appear in more than one group. – For instance; access rights and restrictions to the EHR database have to be defined by policies/routines and it has to be configured. Another example is encryption issues where routines for key administration also have to be defined.

<table>
<thead>
<tr>
<th>Treatment; security measures</th>
<th>Affected threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policies, routines and procedures to be defined for:</td>
<td>g2</td>
</tr>
<tr>
<td>- Installation, upload, and upgrade of Snow sw at GP offices and PO</td>
<td>c2a, c2b, i1a, i1b</td>
</tr>
<tr>
<td>- Access rights and restrictions to EHR database</td>
<td>g2, c2a, c3</td>
</tr>
<tr>
<td>- Administration of encryption keys</td>
<td>c3, a1a, a2, a3a, i1a</td>
</tr>
<tr>
<td>- Security measures and protection at GP office and PO</td>
<td>c1</td>
</tr>
<tr>
<td>- Restriction of results from geographic areas with limited population</td>
<td></td>
</tr>
</tbody>
</table>

8 In this table threats with severe consequence are written in bold face print, while the rest of the threats are written in normal print.
### Treatment; security measures

<table>
<thead>
<tr>
<th>Design and configuration decisions:</th>
<th>Affected threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Access rights/restrictions to EHR database</td>
<td>c2a, c2b, i1a, i1b</td>
</tr>
<tr>
<td>- Database access method (EHR database)</td>
<td>c2a, c2b, i1a, i1b</td>
</tr>
<tr>
<td>- Where to process and aggregate sensitive information</td>
<td>c1</td>
</tr>
<tr>
<td>- Limit the possibility to paste (sensitive) information into messages</td>
<td>c4, c5</td>
</tr>
<tr>
<td>- How to handle GP offices (Snow servers) that do not respond</td>
<td>a6a</td>
</tr>
<tr>
<td>- Strategies for limitation of load</td>
<td>a2, a3a, a3b, a5</td>
</tr>
<tr>
<td>- Filters to restrict communication</td>
<td>a4</td>
</tr>
<tr>
<td>- “Karma” – black-listing of clients</td>
<td>a1a, a3b, a4</td>
</tr>
<tr>
<td>PKI and encryption:</td>
<td></td>
</tr>
<tr>
<td>- Digital signature on installed/uploaded sw modules</td>
<td>g2, c2a, i3b</td>
</tr>
<tr>
<td>- End-to-end encryption of transferred data</td>
<td>c3, i2</td>
</tr>
<tr>
<td>Quality assurance and test procedures</td>
<td>c2b, a1b, a3b, i1b, a8a, a8b</td>
</tr>
<tr>
<td>User education and training:</td>
<td></td>
</tr>
<tr>
<td>- Information on legal aspects and risks; awareness</td>
<td>c4, c5, i3a</td>
</tr>
<tr>
<td>- Good (self-evident) user interface with on-line help</td>
<td>c5, a9</td>
</tr>
<tr>
<td>- Simple user manuals</td>
<td>c5, a9</td>
</tr>
<tr>
<td>- User training/education</td>
<td>c5, a9</td>
</tr>
</tbody>
</table>

For a couple of threats, **risk avoidance** could be an alternative to risk reduction: The threats related to disclosure of sensitive information in messages (threats **c4** and **c5**) could be avoided by not implementing the functionality of sending messages.

**Risk transfer** could be an alternative treatment for a couple of other threats, i.e. pay an insurance to cover for a possible economical loss as a result of an unwanted incident. This could be a solution for threats causing the GPs EHR system to be unavailable for a period of time (**a1a** and **a1b**) and for threats to the integrity of information in the EHR database (**i1a** and **i1b**).

### 4.1.1 Treatment of threats with Medium risk

This section discusses the threats from section 3.2.

**c1** – **Sensitive (i.e. person identifiable) information is extracted from the EHR by the agents, and communicated in the Snow system.**

Anonymisation is imposed, meaning that obviously identifiable information like name, full address, and personal number⁹ are not retrieved from the EHR. It is an open question whether gender, age, or age group should be extracted. But some data could still be sensitive because of small geographic area (municipality, postal code area) and rare diagnosis. Routines must be defined for restrictions with respect to rare diagnoses, limited geographical areas, gender, age, etc. Finally, the doctors should be given the possibility to define/configure which diseases they will (not) provide information about, by defining their own “disease profiles”.

A part of this is to decide where the sensitive information is to be processed, controlled and assembled. Sensitive information could be transferred from GP office to PO if end-to-end

---
⁹ i.e. fødselsnummer
encryption is imposed. But the question is whether the result could be made public if there is only one case in a small population. – Which size should the population have to allow the result to e.g. be shown on a map? (Treatment of this threat is further discussed in Annex C.)

**a3b – Increased load on the local systems at the GP office, and correspondingly decreased responsiveness, because of features in the Snow system.**

Black-listing of clients who send (too) many requests (“Karma”).

Quality assurance and extensive test procedures are needed to avoid programming errors, bugs, wrong configurations, and missing limitations/restrictions. In particular, extensive testing of the Snow system together with a running EHR system should be performed.

There are many ways to restrict this type of load:

- Processing of extensive requests (for a wide time period) could be restricted to be performed only at night time.
- A maximum number of agents per Agent Daemon (configurable). A new agent will not start until there are available resources.
- During outbreaks it is foreseen that many equal requests are submitted at the same time. For this purpose, a cache could be kept in PO for “fresh” results.
- Timeout on unsuccessful actions to avoid deadlock or infinite loop; the corresponding agents are killed.

**4.1.2 Treatment of severe threats with Low risk**

This section discusses the threats from section 3.3.

**g2 – False or bogus software modules can be installed on the Snow servers or in the GP’s local systems.**

Routines must be made for upload, installation, and upgrade of the Snow software to the servers at the GP office (and to the PO). A central part of the solution should be digital signature on the uploaded software. – One could compare this to how the EHR system vendors install and update their software. This is part of the general information security strategy at the GP offices.

The information (spec luggage) sent to the SAS server for a specific mission must not interfere with the SAS software repository. There should be dedicated ports for input/output of such data to/from the server.

**c2a – Sensitive information from the GP’s EHR is revealed to unauthorised persons by false or bogus agents that are able to extract sensitive information from the local EHR.**

This threat is related to threat g2 above: If it is possible to introduce fake/bogus software modules, then they can do all sorts of harm. Access rights to the EHR database must be restricted with respect to which information it is possible to extract. Then the fake/malicious software must also modify the access rights to the EHR database (the configuration).

Different alternatives for database access should be considered. Among these are the use of web services (which is a language independent solution), and a combination of stored procedures and view.

**c2b – Sensitive information from the GP’s EHR is revealed to unauthorised persons because errors/bugs in the Snow software makes it possible to extract sensitive information from the local EHR.**

Quality assurance and extensive test procedures must be performed in order to avoid programming errors. This also includes the configuration of database access.
Access rights to EHR database must be restricted (see c2a above), including the right to modify the configuration. EHR access is limited to the specific application, e.g. epidemiology. A programming error cannot violate that. An agent can not extract more information than what has been defined as accessible.

c3 – Sensitive information is exposed during transfer because of wiretapping, unauthorised persons “listening in” to the communication.

Data transferred between Snow server at GP office and PO will be encrypted end-to-end, by use of PKI solution and session keys. Routines for key administration must be defined. Data will be decrypted in PO, for further processing. This means that the PO must be placed in secured/trusted environments, with protection like firewalls and virus control. This is assumed to be the case if PO is located in the Norwegian health net. (See also discussion of threat c1 in section 3.2 above.)

c4 – The GP intentionally performs a copy-paste operation from the EHR into a message which is submitted to the JID for a receiver.

There is not much to do if the doctor really intends to do this. But measures discussed for c5 below could also reduce the risk for this threat.

c5 – Unintentional delivery of information from GP, caused by an unintentional copy-paste, or by sending a message to a wrong receiver address (JID)

Information should be given to the users (GPs) about legal aspects and the possible risks (awareness). Education and training of users is necessary to avoid user mistakes, combined with good, obvious user interfaces and instructing user manuals.

A more strict measure is to remove the possibility to paste data from EHR into messages. Or, if this functionality is really necessary, have a pop-up dialogue box asking the user for a confirmation of the paste operation, with default set to “no”, and where the text to be pasted is shown in the dialogue box.

A strategy for risk avoidance is to not open up for the possibility to send messages, at least not from the ordinary GPs. This could, however, be a useful functionality for the “disease prevention doctor”.

a1a, a1b – The Snow system crashes the local EHR server, which results in either a disk crash with destroyed data or the EHR system being unavailable for a period of time.

These incidents could be caused by malicious DoS-attack utilizing weaknesses in the Snow system, or by other errors/bugs in Snow. The local system at the GP office is assumed to have an up-to-date information security management system with firewall, virus control, and regular security patching. The information security management system shall also have routines for backup and restore. This should minimize the damage in case of disk crash.

It should also be investigated whether it is possible to retrieve lost messages again from the communication service, i.e. the latest messages, sent after the last backup.

Black-listing should be imposed of clients who send (too) many requests (“Karma”).

Bugs that steal processing time will cause problems for the Snow service but not for the local EHR. Area reserved for each process is normally protected from the area of other processes. We must assume that these types of weaknesses in MS Windows is detected and corrected.

In any case, quality assurance and extensive test procedures is always needed to avoid programming errors.
A different and additional approach could be *risk transfer*: Consider the possibility to pay an insurance to cover for possible economical losses of the GP if the EHR system is unavailable for a period of time.

**i1a, i1b – The Snow system causes modification of data/information and relations in the local EHR system, which results in wrong patient treatment.**

The local system at the GP office is assumed to have an up-to-date information security management system with firewall, virus control, and regular security patching.

As for c2a above, access restrictions must be imposed on the EHR database, by the EHR system vendors. The Snow modules do not need to have write access to the EHR database. Alternatives for database access must be decided (Web Services or a combination of stored procedures and view).

As for c2b above, quality assurance and extensive test procedures must be imposed, to avoid programming errors.

An additional approach could be *risk transfer*: Consider the possibility to pay an insurance to cover for possible economical losses of the GP if damages to the EHR system cause wrong patient treatment.

### 4.2 Further investigations needed

Not all threats could be analysed in this first risk assessment, mainly because of uncertainties in the architecture and design of the Snow system. At such an early stage, threats have been difficult to analyse with respect to consequence and in particular with respect to likelihood.

Most of the threats have got a Low risk level, mainly because the likelihood for these unwanted incidents has been evaluated to be Low. As mentioned above, this is related to the problems of analysing a system which is in its early design phase.

For the following threats we have not at all been able to give a value for likelihood and/or consequence:

- **g1** – Use of open source software, and/or publishing the Snow software as open source. This problem is foreseen to be addressed in a separate study, at a general level.

- **a8a, a8b** – Snow service unavailable as a result of software errors, at the GP office and PO, respectively. It is difficult to predict the likelihood for this, but in any case it is important to impose quality assurance routines and extensive test procedures.

- **a9** – Snow service unavailable as a result of wrong use (wrong user actions) at the GP office. Also for this it is difficult to predict the likelihood; data concerning usage will be needed. In any case it is important to have an intuitive user interface, good user manuals, and training and education of users.

Quality threats **q1-q4** – These threats are mainly related to the coverage of the results: Is the number of participating GPs large enough? Is the resulting information representative of the real situation? There is also a basic question whether these quality threats concerns the information security at all. One argument for keeping them in the risk assessment for information security is that

A second and more thorough risk assessment is needed when the system design is stable and the implementation has been tested to a certain extent. In addition to testing the quality and functionality of the Snow system, tests should be performed related to performance, throughput, and system load. It is particularly important to test the system load when Snow is running together with the EHR system. Paper [6] presents a scalability testing that has been done, but
in that case only the performance of Snow was evaluated, not the performance of an EHR system running with Snow.

Before the next risk assessment there should also be clarifications concerning the expected coverage of the Snow service (number of GP offices participating, geographical area covered), and the responsibilities regarding operations, maintenance and support of the Snow service should be decided.

4.3 Conclusions

In general, it is difficult to assess the information security risk of a system that has not been developed yet, or not even designed. Many threats can be identified as possible unwanted incidents, but it is impossible to foresee their risk level, the consequence, and in particular the likelihood for it to happen.

The main result at this stage is therefore that we have been able to imagine (identify) threats and possible unwanted incidents, and to foresee consequences of these.

In this first risk assessment of the Snow service no threats with an unacceptable High risk level have been identified.

Only two threats have been given a Medium risk level, one of these (c1) is considered to be unacceptable. Threat c1 concerns the possibility that the information produced by the Snow service is sensitive, i.e. not anonymous “enough”.

Among the threats with Low risk level we have focused especially on the threats with severe consequence. The argument for this is that with an increased likelihood these threats will easily get an unacceptable risk level. A tendency, based on consequence, is that all the confidentiality threats have severe consequence, while most of the availability threats have lower consequence. The integrity threats are distributed between severe and moderate consequence.

Measures for risk reduction have been proposed in section 4.1. Among these treatment options we want to mention the following from table 4:

- Definition of policies, routines and procedures for specific areas, like:
  - installation, upload, and upgrade of Snow software modules at GP offices and PO
  - access rights and restrictions to the EHR database
  - administration of encryption keys
  - security measures at GP office and PO (firewall, virus protection, backup, etc)
  - how to restrict results from areas with limited population so that it is still anonymous.

- Design and configuration decisions for e.g.:
  - access to EHR database (access rights and methods)
  - filters to restrict communication and limit system load

- Encryption and PKI – to protect confidentiality and integrity

- Quality assurance and test procedures

- Training and education of users

In section 4.1 we have also mentioned risk avoidance and risk transfer as alternatives to risk reduction for a few of the risks. It is up to the project owners to decide whether these are realistic approaches.
References


[8] Act of 14 April 2000 no. 31 relating to the processing of personal data [Personal Data Act]
   http://www.ub.uio.no/ujur/ulovdata/lov-20000414-031-eng.pdf
   http://www.lovdata.no/all/hl-20000414-031.html

[9] Act on personal health data filing systems and the processing of personal health data [Personal Health Data Filing System Act]
   http://www.lovdata.no/all/hl-20010518-024.html

[10] Act of 2nd July 1999, no 64 relating to health personnel etc. [The Health Personnel Act]
    LOV-1999-07-02-64 – Lov 2. juli 1999 nr. 64 om helsepersonell m.v. (Helsepersonellobyen).
    http://www.lovdata.no/all/hl-19990702-064.html


## Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>AgD</td>
<td>Agent Daemon (in Snow)</td>
</tr>
<tr>
<td>ALARP</td>
<td>As Low As Reasonable Possible</td>
</tr>
<tr>
<td>DoS</td>
<td>Denial of Service</td>
</tr>
<tr>
<td>EHR</td>
<td>Electronic Health Record</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>GP</td>
<td>General Practitioner (doctor)</td>
</tr>
<tr>
<td>HW</td>
<td>Hardware</td>
</tr>
<tr>
<td>ID</td>
<td>Identifier / Identification</td>
</tr>
<tr>
<td>IM</td>
<td>Instant Messaging</td>
</tr>
<tr>
<td>JID</td>
<td>Jabber IDentifier</td>
</tr>
<tr>
<td>MC</td>
<td>Mission Controller</td>
</tr>
<tr>
<td>MUC</td>
<td>Multi-User Chat</td>
</tr>
<tr>
<td>PII</td>
<td>Personal Identifiable Information</td>
</tr>
<tr>
<td>PKI</td>
<td>Public Key Infrastructure</td>
</tr>
<tr>
<td>PO</td>
<td>Post Office (server in Snow)</td>
</tr>
<tr>
<td>QA</td>
<td>Quality Assurance</td>
</tr>
<tr>
<td>SAS</td>
<td>Snow Agent System</td>
</tr>
<tr>
<td>SW</td>
<td>Software</td>
</tr>
<tr>
<td>TCP</td>
<td>Transmission Control Protocol</td>
</tr>
<tr>
<td>UML</td>
<td>Unified Modelling Language</td>
</tr>
<tr>
<td>XML</td>
<td>eXtensible Mark-up Language</td>
</tr>
</tbody>
</table>
**Annex A Threat table**

The following table indicates likelihood, consequence and resulting risk level for each identified threat. (The values actually used in the analysis are indicated in **bold**.)

*General comments, valuable for system design, have been gathered at the end of (below) this table.*

<table>
<thead>
<tr>
<th>ID</th>
<th>Threat / Unwanted incident</th>
<th>Cause</th>
<th>Likelihood</th>
<th>Consequence</th>
<th>Risk level</th>
<th>Comments and descriptions of implemented security measures</th>
</tr>
</thead>
</table>
| **g1** | Open source software  
- use of open source modules  
- making open source sw | ?? | ?? | ?? | To be investigated |
| **g2** | False/fake sw modules can be installed on SAS server or in the GP office’s systems  
- can do “all sorts of harm”, to confidentiality, integrity, availability  
ex.: a false/fake client that sends a request to a false/fake agent that extracts patient id etc from EHR… | **Low** | **Severe**  
for the service, the trust and reputation of Snow | **Low** | Routines for upload, installation and/or upgrade of sw to SAS server at GP offices.  
- Should be compared to how the EHR system vendors install, upgrade and update their sw.  
This is part of the general information security strategy at the GP offices, like firewalls, virus protection, security updates, etc.  
The information (spec luggage) sent to the SAS server for a specific mission must not interfere with the SAS sw repository.  
Solutions? Dig. signature on installed modules |
<table>
<thead>
<tr>
<th>ID</th>
<th>Threat / Unwanted incident</th>
<th>Cause</th>
<th>Likelihood</th>
<th>Consequence</th>
<th>Risk level</th>
<th>Comments and descriptions of implemented security measures</th>
</tr>
</thead>
<tbody>
<tr>
<td>c1</td>
<td>The information extracted from the EHRs by the agents is sensitive, i.e. person identifiable information (not anonymous)</td>
<td>To be further investigated - but &gt;Low if not taken care of in the design, e.g. Moderate?</td>
<td>Severe? - it depends on who sees this information</td>
<td>Medium?</td>
<td>Routines for restrictions of rare diagnoses, limited geographical areas, gender? Anonymisation is imposed, but it is a question whether the transferred information is sensitive or not. – We assume some data could be sensitive due to small geographical area (municipality, postal code area) and rare diagnosis. Where is the information controlled and assembled? Locally at GP or in PO?</td>
<td></td>
</tr>
<tr>
<td>c2a</td>
<td>Worst case: Sensitive information from EHR falls into hands of unauthorised persons</td>
<td>False/fake Agent Daemon (or Agent) that extracts sensitive information from EHR</td>
<td>Low? see g2 above</td>
<td>Severe - serious loss of reputation for service provider and patient</td>
<td>Low</td>
<td>Access to EHR must be limited wrt. which information is possible to extract. The malicious sw must then also modify the access rights to the EHR DB (config.?) Alternatives for database access: - Web Services (language independent), or a combination of stored procedures and view?</td>
</tr>
<tr>
<td>c2b</td>
<td>SW bugs: Erroneous Agent Daemon (or Agent) that extracts sensitive information from EHR</td>
<td>Very Low Can not extract more information than what has been defined as accessible.</td>
<td>Severe</td>
<td>Low</td>
<td>Programming errors: Testing! EHR access limited to the specific application, e.g. epidemiology. A programming error cannot violate that. (Is this a sort of configuration? What if the configuration is wrong – i.e. configuration error? How is the configuration set? Changed? → Routines needed…)</td>
<td></td>
</tr>
<tr>
<td>ID</td>
<td>Threat / Unwanted incident</td>
<td>Cause</td>
<td>Likelihood</td>
<td>Consequence</td>
<td>Risk level</td>
<td>Comments and descriptions of implemented security measures</td>
</tr>
<tr>
<td>----</td>
<td>-----------------------------</td>
<td>-------</td>
<td>------------</td>
<td>-------------</td>
<td>------------</td>
<td>--------------------------------------------------------</td>
</tr>
<tr>
<td>c3</td>
<td>Sensitive information is exposed during transfer</td>
<td>Wiretapping, unauthorised persons “listening in” to the communication (Other ways of doing this?)</td>
<td>Very Low - because data will be encrypted during transfer</td>
<td>Severe</td>
<td>Low</td>
<td>End-to-end encryption during transfer, use of PKI solutions and session keys (TBD). Data is decrypted in PO, for processing. This means that PO must be secured/trusted.</td>
</tr>
<tr>
<td>c4</td>
<td>Intentional, but unauthorised, delivery of information</td>
<td>The GP does an intentional copy-paste operation from the EHR into a Jabber message and sends it to the JID for the receiver</td>
<td>Low? But this is a new tool that makes it easier to send info</td>
<td>Severe</td>
<td>Low</td>
<td>This is the same threat as for other services (e.g mail) available for the GP. - Could remove the possibility to paste data from EHR into messages? - Or a pop-up dialogue box asking the user for a confirmation of the paste operation, with default = &quot;no&quot; – and showing the text to be pasted.</td>
</tr>
<tr>
<td>c5</td>
<td>Unintentional delivery of information</td>
<td>Unintended copy-paste, or sending to the wrong JID</td>
<td>Low? - remains to be seen…</td>
<td>Severe</td>
<td>Low</td>
<td>(As above.)</td>
</tr>
<tr>
<td>ID</td>
<td>Threat / Unwanted incident</td>
<td>Cause</td>
<td>Likelihood</td>
<td>Consequence</td>
<td>Risk level</td>
<td>Comments and descriptions of implemented security measures</td>
</tr>
<tr>
<td>----</td>
<td>----------------------------</td>
<td>-------</td>
<td>------------</td>
<td>-------------</td>
<td>------------</td>
<td>---------------------------------------------------------</td>
</tr>
</tbody>
</table>
| a1a| **Worst case**: The SAS system crashes the local EHR server (or the database)  
This is a wide problem, the result could be different:  
a) Disk crash with destroyed data  
b) System/service is down for a period of time | DoS-attack (intentional) | Low | Severe? due to loss of reputation and trust | Low | “Karma” – “black listing” of clients who sends (too) many requests. If disk crash: The GP office will/shall have an information security management system with necessary routines for e.g. backup. – Could it also be possible to have routines for retrieval of lost messages from the communication service? (Recent messages, after the last backup.) |
| a1b| | Erroneous sw, bugs e.g. that steal processing time and resources, e.g. never free memory… | Low | Severe? due to loss of reputation and trust | Low | Testing, test procedures, input verification. Bugs that steal processing time will cause problems for Snow but not for the local EHR. Area reserved for each process is normally protected from other’s area. Must assume that these kinds of weaknesses in Windows is detected and corrected… |
| a2 | DoS-attack crashes the Snow system | Malicious action from "internal" *(i.e. internally in the Snow service…)*  
(One way to do this is to repeat a request for data from a very long time period.) | Low | Moderate - maybe worse if the GPs are being dependant of Snow’s functionality | Low | Motivation? E.g. to prevent a successful service or a successful result of the project…  
*How will this be discovered from the outside (from support)? PO performs a status control by frequent polling and logs and reports the (missing) responses.*  
Post office will have the first pressure if the attack comes from the outside. PO can be more powerful than the computers at the GP offices. PO must control the amount of requests that are being forwarded, e.g. one at the time? (Or queuing at the GP server?) |
<table>
<thead>
<tr>
<th>ID</th>
<th>Threat / Unwanted incident</th>
<th>Cause</th>
<th>Likelihood</th>
<th>Consequence</th>
<th>Risk level</th>
<th>Comments and descriptions of implemented security measures</th>
</tr>
</thead>
<tbody>
<tr>
<td>a3a</td>
<td>Increased load on local system that significantly decreases the responsiveness</td>
<td>DoS-attack (intentional)</td>
<td>Low</td>
<td>Moderate</td>
<td>Low</td>
<td>See above, a1a and a2. A DoS-attack does not necessarily crash the system; but it may overload it.</td>
</tr>
<tr>
<td>a3b</td>
<td></td>
<td>SW features, e.g. too many missions/requests and corresponding agents executing simultaneously.</td>
<td>High</td>
<td>Moderate</td>
<td>Medium</td>
<td>Errors, bugs, wrong configuration, etc. Missing limitations/restrictions. Many ways to restrict this type of load. – Could for instance restrict extensive requests (for a wide time period) to be performed only at night time. Max number of agents per Agent Daemon (configurable). A new agent will not start until there are available resources. E.g. during outbreaks: Many equal requests submitted at the same time. Cache in PO for “fresh” results. (What if the requests are different?) Testing: What is the system load? Deadlock or infinite loop: Timeout on unsuccessful actions, the corresponding agents are killed. Filters (in PO) to limit how widely the JID should be known. Filter to restrict who could contact these JIDs. (Karma… see a1a above)</td>
</tr>
<tr>
<td>a4</td>
<td>Unauthorised persons communicates with local Jabber server → increased load on system</td>
<td>JID for the Agent and Agent Daemon is known externally (sort of DoS-attack)</td>
<td>Low</td>
<td>Moderate</td>
<td>Low</td>
<td>The JID is available only inside the “closed” system, i.e. inside the health net. No relevant communication from Internet into the health net. (Only well-defined application proxy- and relé-based services are let through the firewall.) Filters (in PO) to limit how widely the JID should be known. Filter to restrict who could contact these JIDs. (Karma… see a1a above)</td>
</tr>
<tr>
<td>ID</td>
<td>Threat / Unwanted incident</td>
<td>Cause</td>
<td>Likelihood</td>
<td>Consequence</td>
<td>Risk level</td>
<td>Comments and descriptions of implemented security measures</td>
</tr>
<tr>
<td>----</td>
<td>-----------------------------</td>
<td>-------</td>
<td>------------</td>
<td>-------------</td>
<td>------------</td>
<td>-------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| a5 | Undue consumption of storage space in local system | Storage of old data/information | Low | Moderate | Low | - AgD will monitor the need for disk space and compare with the available disk space, before a new agent is launched. 
  - The disk will fill up quicker, and some applications could stop working. |
| a6a | SAS service unavailable due to other technical problems: - Network problems | - at GP office | Moderate | Small? | Low | - Has a certain consequence for reputation, trust in the service. 
  - Snow would assume that all GP offices are connected. 
  - Approx. 80% of GP offices in the pilot region are "always connected" (20% still ISDN). 
  - Standard SLA for Wanda-connected GP offices guarantees 99.5% availability on a monthly basis. 
  - Could skip the GP offices that do not respond, and/or do a retry on them later on in the round. 
  - The coverage or completeness ("sensitivity") of the result should be stated, i.e. the amount of GP offices that are included. |
<table>
<thead>
<tr>
<th>ID</th>
<th>Threat / Unwanted incident</th>
<th>Cause</th>
<th>Likelihood</th>
<th>Consequence</th>
<th>Risk level</th>
<th>Comments and descriptions of implemented security measures</th>
</tr>
</thead>
<tbody>
<tr>
<td>a6b</td>
<td>- at PO (in health net)</td>
<td>Low - less likely that the PO is not connected?</td>
<td>Moderate - The PO and all the GPs in its area will be out of reach</td>
<td>Low</td>
<td>Has a certain consequence for reputation, trust in the service.</td>
<td></td>
</tr>
<tr>
<td>a7a</td>
<td>SAS service unavailable due to other technical problems: - HW failures</td>
<td>- at GP office</td>
<td>Low? Would assume that the GP offices have support contracts to deal with hw problems quickly</td>
<td>Small? - for the Snow service - it is not caused by Snow…</td>
<td>Low</td>
<td></td>
</tr>
<tr>
<td>a7b</td>
<td>- at PO</td>
<td>(Very) low Less likely?</td>
<td>Moderate - The PO and all the GPs in its area will be out of reach</td>
<td>Low</td>
<td>Has a certain consequence for reputation, trust in the service.</td>
<td></td>
</tr>
<tr>
<td>a8a</td>
<td>SAS service unavailable due to other technical problems: - SW errors</td>
<td>- at GP office</td>
<td>Difficult to predict…</td>
<td>Moderate? Or severe? Such errors will most likely exist in all GP installations</td>
<td>??</td>
<td>Has a certain consequence for reputation, trust in the service. Extensive testing and QA during the development process.</td>
</tr>
<tr>
<td>a8b</td>
<td>- at PO</td>
<td>Difficult to predict…</td>
<td>Moderate - The PO and all the GPs in its area will be out of reach</td>
<td>??</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Side 32 av 40
<table>
<thead>
<tr>
<th>ID</th>
<th>Threat / Unwanted incident</th>
<th>Cause</th>
<th>Likelihood</th>
<th>Consequence</th>
<th>Risk level</th>
<th>Comments and descriptions of implemented security measures</th>
</tr>
</thead>
<tbody>
<tr>
<td>a9</td>
<td>SAS service unavailable due to other technical problems: - Erroneous user actions</td>
<td>- at GP office</td>
<td>Difficult to predict… will need data about usage</td>
<td>Small</td>
<td>Will hit only one GP office?</td>
<td>??</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>i1a</td>
<td>Worst case: The SAS service modifies data/information and relations in the EHR system, which causes modification to patient treatment.</td>
<td>False/fake sw modules (i.e. malicious sw)</td>
<td>Low?? (What should be the motivation?)</td>
<td>Severe</td>
<td>Low</td>
<td>The Snow modules do not need to have write access to the EHR database. This threat depends on which access rights that the EHR provider (here: Profdoc) give to Snow.</td>
</tr>
<tr>
<td>i1b</td>
<td></td>
<td>SW bugs/errors in the Snow system</td>
<td>Low? - difficult to predict.</td>
<td>Severe</td>
<td>Low</td>
<td>Encryption procedures – to be investigated Is it more serious if it is the requests that are being modified?</td>
</tr>
<tr>
<td>i2</td>
<td>Data (Snow results) is being modified during transfer</td>
<td>- deliberately, by intruders in the network</td>
<td>Very Low</td>
<td>Moderate</td>
<td>Low</td>
<td></td>
</tr>
<tr>
<td>i3a</td>
<td>Production of false results from Snow</td>
<td>Wrong/fake info inserted in the EHR - deliberately (done by the GP?)</td>
<td>Low</td>
<td>Moderate</td>
<td>Low</td>
<td>Could cause panic… It is not possible for an outsider to join the system as a new GP office. It has to be managed in the PO etc, it has to be registered. Means that there is an admin job to be done for the PO and Main. - It is not possible for a fake GP to be connected to NHN and registered in HER. Before a GP is connected to the Health Network, the 9-digit business ID is verified against the national register in Brennøysund, and a check is also performed against the Fastlege directory. - The client receives the result and interprets and presents it (in a map) → the client must verify the origin of the result (the sender)</td>
</tr>
<tr>
<td>i3b</td>
<td></td>
<td>False/fake clients, users or agents - the client can for instance receive the fake/false result as a chat message?</td>
<td>Low? (What should be the motivation?)</td>
<td>Moderate</td>
<td>Low</td>
<td></td>
</tr>
</tbody>
</table>

**Integrity**
<table>
<thead>
<tr>
<th>ID</th>
<th>Threat / Unwanted incident</th>
<th>Cause</th>
<th>Likelihood</th>
<th>Consequence</th>
<th>Risk level</th>
<th>Comments and descriptions of implemented security measures</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Data quality</td>
<td>Must consider whether these threats really concerns information security… For further study – evaluation.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>q1a</td>
<td>Data from a limited set of GPs</td>
<td>“All” the GP offices (EHRs) are not online</td>
<td>??</td>
<td>??</td>
<td>??</td>
<td>EHR must be online 24/7 ? see above a6a</td>
</tr>
<tr>
<td>q1b</td>
<td>Data from a limited set of GPs</td>
<td>Too few GPs participates in the system because they do not trust/believe in the service</td>
<td>??</td>
<td>??</td>
<td>??</td>
<td>Motivation… Indicate the amount of GP offices participating, from system logs. Could also be done before the request: - Indicate the amount that is configured to “no”/”yes” for optional. Then the requester could determine if it is useful to launch the mission or not…</td>
</tr>
<tr>
<td>q2</td>
<td>Too old data</td>
<td>“All” the GP offices (EHRs) are not online</td>
<td>??</td>
<td>??</td>
<td>??</td>
<td>Data freshness: GP must be aware of how old/fresh the resulting information is. Cache routines to be defined. EHR must be online 24/7 ? See above a6a</td>
</tr>
<tr>
<td>q3</td>
<td>Data correctness is low</td>
<td>?? Misinterpretation of info, e.g. when performing free text search</td>
<td>??</td>
<td>??</td>
<td>??</td>
<td>GP’s report to be afraid of getting “too many false positive”. Depends on use of correct code for diagnosis and symptom and that the GP updates the code in the EHR when it is confirmed from e.g. lab results.</td>
</tr>
</tbody>
</table>

Other threats
**Annex B Plan for implementation of security measures**

Proposed measures for threats with risk level *Medium* and threats with severe consequence are listed in the following table. The table should be used in the follow-up of the risk treatment.

<table>
<thead>
<tr>
<th>ID</th>
<th>Threats, unwanted incidents</th>
<th>Security measures</th>
<th>Responsible</th>
<th>Deadline</th>
<th>Status</th>
</tr>
</thead>
</table>
| g2 | False/fake software modules can be installed on the Snow servers or in the GP’s local systems | Routines for upload, installation, and upgrade of Snow sw to servers at the GP office (and to the PO)  
Digital signature on the uploaded sw.  
Spec luggage to the SAS server for a specific mission must not interfere with the SAS sw repository. Dedicated ports for input/output of such data to/from the server. | | | |
| c1 | Sensitive information is extracted from the EHR by the agents, and communicated in the Snow system | Routines for restrictions of rare diagnoses, limited geographical areas, gender, etc.  
E.g. decide where the sensitive information is to be controlled and assembled: Locally at GP or in PO? | | | |
| c2a | Sensitive information from the GP’s EHR is revealed to unauthorised persons by false/fake agents that are able to extract sensitive information from the local EHR | Access restrictions imposed on the EHR database. – This must be handled by the EHR system vendors. This also includes the possibilities to modify access rights (configuration).  
Decide on alternatives for database access:  
- Web Services (language independent)  
- combination of stored procedures and view | | | |
<table>
<thead>
<tr>
<th>ID</th>
<th>Threats, unwanted incidents</th>
<th>Security measures</th>
<th>Responsible</th>
<th>Deadline</th>
<th>Status</th>
</tr>
</thead>
</table>
| c2b | Sensitive information from the GP’s EHR is revealed to unauthorised persons because errors/bugs in the Snow software makes it possible to extract sensitive information from the local EHR | Same as for c2a above.  
Plus:  
Quality assurance and extensive test procedures to avoid programming errors. | | | |
| c3 | Sensitive information is exposed during transfer because of wire-tapping, unauthorised persons “listening in” to the communication | End-to-end encryption of transferred data between Snow server at GP and PO, using PKI solution and session keys.  
Routines for key administration have to be defined.  
Protection of PO, like firewall and virus protection. Data is decrypted in PO, for processing, so PO must be placed in a secured/trusted environment. This is assumed to be in place if PO is located in the Norwegian health net. | | | |
| c4 | The GP *intentionally* performs a copy-paste operation from the EHR into a message which is submitted to the JID for a receiver | Information to users about legal aspects and possible risks (awareness). Education and training of users. Good user interfaces, user manual. | | | |
| c5 | Unintentional delivery of information from GP, caused by an unintentional copy-paste, or by sending a message to a wrong receiver address (JID) | Remove the possibility to paste data from EHR into messages. – Or have a pop-up dialogue box asking the user for a confirmation of the paste operation, with default = “no” – and showing the text to be pasted.  
A more strict approach to these threats is risk avoidance: Do not implement the possibility to send messages. | | | |
<table>
<thead>
<tr>
<th>ID</th>
<th>Threats, unwanted incidents</th>
<th>Security measures</th>
<th>Responsible</th>
<th>Deadline</th>
<th>Status</th>
</tr>
</thead>
</table>
| a1a| A DoS attack through the Snow system crashes the local EHR server, which results in either a disk crash with destroyed data or the EHR system to be unavailable for a period of time | The local system at the GP office is assumed to have an up-to-date information security management system with firewall, virus control, and regular security patching.  
The information security management system shall also have routines for backup and restore. This should minimize the damage in case of disk crash.  
Black-listing of clients who sends (too) many requests ("Karma").  
Quality assurance and extensive test procedures to avoid programming errors.  
*Risk transfer* is a different (and additional?) approach: Pay insurance to cover for possible economical losses of the GP if the EHR system is unavailable for a period of time. |             |          |        |
| a1b| The local EHR server crashes because of errors/bugs in the Snow system, which results in either a disk crash with destroyed data or the EHR system to be unavailable for a period of time |                                                                                       |             |          |        |
| a3b| Increased load on the local systems at the GP office, and correspondingly decreased responsiveness, because of features in the Snow system | Black-listing of clients who sends (too) many requests ("Karma").  
Quality assurance and extensive test procedures to avoid programming errors, bugs, wrong configurations, and missing limitations/ restrictions.  
Ways to reduce load:  
- Extensive requests (for a wide time period) to be processed only at night time.  
- Max number of simultaneous agents per Agent Daemon (configurable).  
- Cache the "fresh" results in PO, for reuse.  
- Timeout on unsuccessful actions, and kill the corresponding agents. |             |          |        |
<table>
<thead>
<tr>
<th>ID</th>
<th>Threats, unwanted incidents</th>
<th>Security measures</th>
<th>Responsible</th>
<th>Deadline</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>i1a</td>
<td>Malicious sw introduced through the Snow system causes modification of data/information and relations in the local EHR system, which results in wrong patient treatment</td>
<td>The local system at the GP office is assumed to have an up-to-date information security management system with firewall, virus control, and regular security patching. As for c2a and a2b above: Access restrictions must be imposed on the EHR database, by the EHR system vendors. The Snow modules do not need to have write access to the EHR database. Alternatives for database access must be decided (Web Services or a combination of stored procedures and view). Quality assurance and extensive test procedures must be imposed, to avoid programming errors. Additionally, consider to pay insurance to cover for possible economical losses of the GP if the EHR system is modified so that it causes wrong patient treatment (<em>risk transfer</em>).</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>i1b</td>
<td>Errors/bugs in the Snow system causes modification of data/information and relations in the local EHR system, which results in wrong patient treatment</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Annex C Design issues related to privacy and security

C.1 Preserve privacy of data from a small data set

The discussion in this section is related to threat c1 – “Sensitive (i.e. person identifiable) information is extracted from the EHR by the agents, and communicated in the Snow system.”

This is the scenario: In a search for diagnosis/disease XY (e.g. HIV…) the agent of a local GP server returns the result “Number of cases in area 1234 is: 1”. And everyone knows that in area 1234 there are only 345 inhabitants. If in addition the gender and/or age are given, the number to choose from is much smaller. And if the number of cases changes at the same time as newcomers arrive to the area, this can be related.

The result to be presented at the end is the aggregated information for e.g. the whole city or county, but before it is aggregated it is transferred as a single result. How can we ensure that the receiver of the single information (or a “hacker” who eavesdrop the communication) is not able to “guess” the identity of this unfortunate person?

The system must not allow presentation of information which is person identifiable in any ways. This can be avoided by necessary consideration taken during design of the information collection functionality and/or the result presentation functionality.

Collection of information:

There are two possible ways to collect the information from all the Snow “members”: Jump or Spread. Figure C1 illustrates the two methods. Because of the communication delay the Jump method is assumed to take longer time, while the Spread method gives a more instant view of the situation.

Using the Spread method, each node (GP Snow server) will return his single result; the result can be identified at the initiating node, or by an eavesdropper. Using the Jump method, each node will see the aggregated result from the preceding nodes. So still the second node will see the result of the first node… One way to prevent this is to initiate the request with a random “salt” value: The initiator starts the round with a random value, the next node adds his result to this value, and so on, and finally the initiator subtracts the “salt” value from the aggregated
value he receives at the end. A random “salt” value can also be used in the Spread case, this
could prevent any eavesdropper from knowing the single result (… unless he also eavesdrop
the request and reads the “salt” value…). But the initiator will still be able to identify the
result from each single node.

Encryption can further protect eavesdropping. By use of asymmetric encryption (PKI), the
information is encrypted with the public key of the receiver (which is found in his certificate).
For the Jump method, this would be the public key of next node. For the Spread method this
will be the public key of the initiator. It depends on who should perform the aggregation, and
therefore needs to decrypt the information.

By use of XML encryption one can choose to encrypt only parts of the message. The same is
the case for digital signing parts of the XML message.

For further study:

Here is another problem that should be discussed, but is too big to be solved in this project:

Independent of Jump or Spread method – how can we be sure that the same person/case is not
counted twice – without communicating the person’s ID? The same case can be registered in
an (active) EHR both at the person’s GP, at the emergency unit, and at the laboratory.

Gustav sketched a special pseudonymisation solution: Each person id (e.g. “personnr”) is
mapped to a set of pseudonyms, as indicated in the table below. *(The size of n needs to be
discussed – do we really need one per site, or can we reuse pseudonyms, e.g. choose among
ten different?)*

<table>
<thead>
<tr>
<th>Person ID</th>
<th>Pseudonym 1</th>
<th>Pseudonym 2</th>
<th>Pseudonym 3</th>
<th>…</th>
<th>Pseudonym n</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>PA1</td>
<td>PA2</td>
<td>PA3</td>
<td>…</td>
<td>PAn</td>
</tr>
<tr>
<td>B</td>
<td>PB1</td>
<td>PB2</td>
<td>PB3</td>
<td>…</td>
<td>PBn</td>
</tr>
</tbody>
</table>

Each site gets one of these pseudonyms for the person. When one node returns his result of a
request, he could include the pseudonym(s) for the individuals. For example:

Node 1 says: - Number of cases: 1 - Pseudonyms: PA2
Node 2 says: - Number of cases: 2 - Pseudonyms: PA6, PB3
Node 3 says: - Number of cases: 1 - Pseudonyms: PA1

The initiator (PO) says: - Total number of cases: 2 (because he knows that PA1, PA2 and
PA6 refer to the same person.)
Report from risk assessment no. 2

The SNOW project

Version 1.0
02.08.2010

Eva Henriksen, Johan Gustav Bellika, Per Atle Bakkevoll, Lars Ilebrekke, Marit Wiklund

Norwegian Centre for Integrated Care and Telemedicine
Summary

The project

The purpose of the Snow service for epidemiology is early detection of disease outbreak, fast and easy notification and management of disease outbreaks. This version of Snow collects its input data from hospital laboratory tests.

In this phase of the project it is also a tool to investigate the research questions in the project, e.g. how the system is used.

The risk assessment

The main part of this risk assessment was performed in April – June 2010. The following persons participated in the risk assessment:
- Risk assessment leader: Eva Henriksen.
- Project participants: Johan Gustav Bellika, Lars Ilebrekke, Per Atle Bakkevoll, and Marit Wiklund (microbiology laboratory, UNN)

To analyse the security challenges of the Snow project, we performed a qualitative risk analysis of the information security aspects of the Snow system as it is implemented now, and the intended environment and use by the microbiology lab at UNN. The goal was to identify security threats to the institutions involved and to patient information, and to find acceptable solutions to the threats. The threats were identified and analysed in six brainstorming sessions, where elements of Fault Tree Analysis (FTA) also were used in the threat identification process.

We performed the risk analysis by going through the five main steps described in the Australian and New Zealand standard for risk management [3].

1. Context identification
2. Threat identification
3. Analysis of the identified threats with respect to likelihood and consequence
4. Calculation of risk value for each threat as the product of consequence and likelihood, illustrated in a two-dimensional matrix
5. Proposal of risk-reduction treatment for all threats with a non-acceptable risk level

This methodology corresponds very well to the international standard ISO 27005 for information security risk management [4].

Main conclusions

This second risk assessment of the Snow system identified two threats with an unacceptable High risk level (q1.1 and c3). Six threats were given a Medium risk level, and five of them (a2, i2, q1.2, q1.3, and q5.1) were evaluated to be unacceptable.

Among the threats with Low risk level, we focused especially on the eleven threats with severe consequence.
TABLE OF CONTENT

SUMMARY .................................................................................................................. 2

The project .................................................................................................................. 2
The risk assessment ..................................................................................................... 2
Main conclusions ....................................................................................................... 2

1 INTRODUCTION ..................................................................................................... 4

1.1 BACKGROUND ..................................................................................................... 4
1.2 RISK ASSESSMENT METHOD ........................................................................... 4

2 CONTEXT IDENTIFICATION ............................................................................... 5

2.1 SECURITY REQUIREMENTS ............................................................................. 5
  2.1.1 Legal baseline .............................................................................................. 5
  2.1.2 Requirements to the Snow service ................................................................. 6
2.2 DESCRIPTION OF SYSTEM AND SERVICE .................................................. 7
  2.2.1 System overview ......................................................................................... 7
  2.2.2 User registration and logging ...................................................................... 8
  2.2.3 Maintenance ............................................................................................... 8
2.3 DEFINITION OF LIKELIHOOD, CONSEQUENCE AND RISK LEVELS .......... 8
  2.3.1 Likelihood and consequence levels ................................................................. 8
  2.3.2 Acceptance criteria ...................................................................................... 10
  2.3.3 Risk levels ................................................................................................... 10

3 THREAT IDENTIFICATION AND ANALYSIS OF RISK ..................................... 12

3.1 THREATS WITH HIGH RISK LEVEL ............................................................ 13
3.2 THREATS WITH MEDIUM RISK LEVEL ....................................................... 13
3.3 THREATS WITH LOW RISK LEVEL ............................................................... 14

4 CONCLUSIONS AND RECOMMENDATIONS .............................................. 16

4.1 RECOMMENDED RISK TREATMENT ......................................................... 16
  4.1.1 Treatment of threats with High risk .............................................................. 17
  4.1.2 Treatment of threats with Medium risk ....................................................... 18
  4.1.3 Treatment of severe threats with Low risk ................................................. 18
4.2 CONCLUSIONS ............................................................................................... 20

REFERENCES ........................................................................................................... 21

ABBREVIATIONS ...................................................................................................... 23

ANNEX A THREAT TABLE .................................................................................... 24

ANNEX B PLAN FOR IMPLEMENTATION OF SECURITY MEASURES ............... 31
1 Introduction

1.1 Background

A first risk assessment of the Snow service was performed in October-November 2007, in the design phase of the project [13]. It was then decided to perform a second and more thorough risk assessment when the system was implemented and tested to a certain extent.

The current report presents the results of the second and more detailed risk assessment of the Snow service which was performed in the spring of 2010.

1.2 Risk assessment method

Risk analysis of information security is a basic requirement of ISO 27002 (formerly ISO 17799), internationally recognized as “the generic information security standard” [1]. Risk analysis is also required by national legislation as a vital part of an information security management system for any organisation. Risk analysis is performed with respect to the main information security aspects Confidentiality, Integrity and Availability. Norwegian legislation for personal health information [9] also includes Quality among the information security aspects. The risk acceptance criteria are defined by the information security policies of the affected organisation.

There are many methods and guidelines for how to perform risk analysis, but all of them include the central tasks of:

- identifying the threats or possible unwanted incidents
- analysing the impacts and probabilities of these threats
- evaluate risks with respect to the acceptance criteria

The method we use is based on our work in the EU-funded research project CORAS from the fifth framework programme (FP5) of Information Society Technology (IST) [2] where a methodology for risk analysis was developed and tested on e-health systems. The methodology was based on the Australian and New Zealand standard for risk management (AS/NZS 4360/1999) [3], which clearly sets out the risk analysis process in five main steps:

1. Context identification; a description of the subject for analysis, i.e. the analysed system and its environment.
2. Threat identification; identify what could possibly happen.
3. Impact and probability analysis; a consideration of the consequences of the threats and the likelihood that these consequences may occur.
4. Risk evaluation; relating the resulting risk level with risk acceptance criteria.
5. Risk treatment; identification and assessment of treatment options.

2 Context identification

The Snow system is a peer-to-peer system that potentially can be used for exchange of any kind of information between health institutions. This risk assessment will only consider a concrete installation of the system that provides health workers with disease statistics. The statistics are based on data from the microbiology laboratory at UNN. In the Snow system, the exported data from the laboratory is categorized and aggregated to provide reports to the health workers. Anyone that has access to the Norwegian Health Net (NHN) can navigate to the web page and look at the disease statistics for Troms and Finnmark.

End user communication is a key feature of the Snow system concepts, but in this concrete installation that functionality will be disabled. It is only used on the system level to prepare the reports for the users. Thus, a user can only see the reports the system has been configured to prepare by the system administrator. More information about the Snow concepts are provided in the published papers [5] and [6], and in the reports listed on the project’s web site.

2.1 Security requirements

Privacy is always an issue when patient data is involved. Protection of patient privacy is therefore an important issue to address for a disease surveillance system [6].

2.1.1 Legal baseline

Privacy requirements related to communication of sensitive patient-identifiable information establish the baseline for the information security needs. Confidentiality requirements originate from the professional secrecy and non-disclosure agreement imposed to all healthcare workers. Requirements to electronic communication of patient information come from national legislation in European countries, which are also based on EU’s regulation on processing of personal data (Directive 95/46/EC) from 1995 [7]. At the lowest level these requirements become apparent through the security policies of the affected organisation.

According to Norwegian legislation, all health-related information concerning an identifiable person is considered sensitive information (Personal Data Act (Personopplysningsloven) §2) [8]. No one else than those who have a treatment relation to the person, should be able to access this person’s health information, unless the patient has given his or her consent.

Norwegian legislation requires risk assessment as part of an information security management system for any organisation. The legislation also defines information security to include the following aspects: Confidentiality, Integrity, Quality, and Availability [8, 9]. The risk assessment is performed with respect to these information security aspects.

Personal identifiable information (PII) is any information that can identify a physical/natural person. The definition of personal information in the EU Directive [7] reads: “Personal data shall mean any information relating to an identified or identifiable natural person (“data subject”); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity”.

The “Article 29 group” is a “working party on the protection of individuals with regard to the processing of personal data”. It has been formed with the regard to the EU Directive [7], in

1 http://www.telemed.no/opensource/snow
2 http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/index_en.htm
particular with regard to Article 29 and paragraph 1(b) of Article 30. (Hence the chosen short-
name.) – In [11] the “Article 29 group” analyses further the concept of Personal Data. They
state that "a person may be identified directly by name or indirectly by a telephone number, a
car registration number, a social security number, a passport number or by a combination of
significant criteria which allows him to be recognized by narrowing down the group to which
he belongs (age, occupation, place of residence, etc.)". This indicates that it also depends on
the context of the particular situation which identifiers are sufficient to achieve identification.

On the other hand, if the information is anonymous it is not defined as personal identifiable
information and not subject to the legislation given by the EU Directive [7] or the Norwegian
Personal Data Act [8].

The Article 29 group defines anonymous data as any information relating to a natural person
where the person can not be identified, neither by the data administrator nor by any other
person, neither directly or indirectly. They state that a hypothetical possibility to single out the
individual is not enough to consider the person as “identifiable”: If, taking into account “all
the means likely reasonably to be used by the controller or any other person”, that possibility
does not exist or is negligible, the person should not be considered as “identifiable”, and the
information would not be considered as “personal data”.

One example: The description “gender: Male; age: 50-59; occupation: Bus driver” is
anonymous if we consider the whole population of Norway, or even Oslo. But if we consider
the population of a small municipality of less than 1000 inhabitants, this could point directly
to one specific person.

If the intention is to keep the information anonymous, the Article 29 group states: If a
criterion appears to lead to identification in a given category of persons, however large (i.e.
only one doctor operates in a town of 6000 inhabitants), this “discriminating” criterion
should be dropped altogether or other criteria be added to “dilute” the results on a given
person.

The Article 29 group concludes that the assessment of whether the information can be
considered as anonymous, or the data identifies an individual, depends on the circumstances.
A case-by-case analysis is therefore needed. Further, they state that: This is particularly
relevant in the case of statistical information, where despite the fact that the information may
be presented as aggregated data, the original sample is not sufficiently large and other pieces
of information may enable the identification of individuals.

2.1.2 Requirements to the Snow service

The information handled by the Snow system is health-related information. Consequently, if
the information is person identifiable (i.e. not anonymous) it will also be sensitive.

A core privacy principle in the design of the Snow system is to keep the sensitive person
identifiable health data locally in each secure system, in this case the laboratory system,
and not transfer it to a central site for processing [5]. Information processing is done locally, and
only anonymous information is communicated by Snow.

The challenge is to insure that the information is anonymous. One thing is to remove
demographical and geographical information that can identify a person directly or indirectly,
such as name, address, telephone number, social security number, passport number, etc. But a
person may also be recognized by narrowing down the group to which he belongs (age, place
of residence, occupation, etc.). For Snow the “narrowing down” is especially related to the

---

3 Refer to the bus driver example in section 2.1.1
size of the population in the selected geographical area (e.g. covering one postal code zone) and to the infrequency of the diagnosis (prevalence).

2.2 Description of system and service

2.2.1 System overview

Figure 1 shows the network boundaries, the servers that are part of the current installation and the flow of data and reports.

![Diagram of network boundaries and servers](image)

**Figure 1: Installation view**

The three network boundaries are the hospital (lab network), health network (NHN) and local networks (GP office/UNN). As part of the installation, the Lab Snow server has been installed in the DMZ of the hospital and the PO server in the health net. The lab database is where all the data are exported from. No calls are made from the DMZ and into the lab database, the lab database decides when and what to export to a specific folder on the Lab Snow server. The users are shown on the right side of the figure. They can access the web services and a web page through port 80 on the PO server. By using the web client uploaded when they navigate to the correct web page, reports from the ReportDB can be loaded for viewing. The users can reach the web services and the ReportDB on the PO server, but nothing else in the system.

The remaining parts of the figure show how communication between the Lab Snow server and the PO server is enabled. More specifically, it shows how new reports are created and inserted into the ReportDB. This is where most of the Snow system components are used. On each of the two servers there is an XMPP server called Openfire. The communication channel between the two servers is using this XMPP server support and sets up transport level security (TLS). Each server has a certificate which is used as part of the authentication process. In the PO server there is a Snow component called Mission Scheduler that decides what reports to create and when to create them. It uses the Snow system to send the query for a report to the Lab Snow server, which starts up a Lab Agent to create the report that was asked for. The Lab Agent retrieves relevant data records from the SnowDB and aggregates

---

4 PO is an abbreviation for Post Office and is explained in the reports about the Snow system.
5 For more description about the Snow components (Agent Daemon, Mission Controller, Agents), see the report from first risk assessment [13]
7 Project web page: [http://www.igniterealtime.org/projects/openfire/index.jsp](http://www.igniterealtime.org/projects/openfire/index.jsp)
them to produce the reports. Finally the new report is sent back to the PO server and stored in the ReportDB.

The SnowDB can be regarded as the systems knowledge base and is updated once a day with new exported data from the lab database. The Import Manager application is responsible for reading the data files, categorizing them by applying specific rules and then saving the relevant data in the SnowDB. The patient ID and requester ID from the data records in the lab database are pseudonymized in the export. It is done by SHA hashing the identifiers before the records are exported. This ensures that the exported data cannot be traced back to a person. However, because a record contains information like age, sex, sample date and zip code, it can still identify a person in a low population. When the LabAgent aggregates the data, certain rules ensure that the end report does not contain the details that enable identification. Therefore the information in the ReportDB can be considered anonymous and thus not sensitive information. This means that the Lab Snow server has data that needs confidentiality protection, but this is not of equal importance on the PO server.

2.2.2 User registration and logging

For research purposes, all actions a user makes in the web client are logged on the PO server. A user does not need to register or log in, but an ID will be generated in order to distinguish users. For recruitment purposes the web client also has support for user registration. The information that can be registered is the user's name, organization/company and e-mail address.

2.2.3 Maintenance

The Lab Snow server is supported by HN IKT. This means that the Snow team only needs to manage the applications installed as part of the system. The PO server, on the other hand, needs to be managed by the Snow team both in terms of server maintenance and application maintenance.

In terms of data quality, the health workers need to have confidence that the reports contain what they claim. Thus, the Snow team needs to have a close collaboration with the laboratory. New analysis codes are created regularly and since these are explicitly specified in the export script from the lab database, none of these records will reach the Snow system unless HN IKT is told about the new codes and can update the export script. In addition, the Snow team must be able to recognize when new codes show up in the export to properly categorize them and ensure that the reports are updated.

2.3 Definition of likelihood, consequence and risk levels

We have chosen to use qualitative values for likelihood, consequence and risk levels.

2.3.1 Likelihood and consequence levels

We decided to use four levels for identification of likelihood and four levels for identification of consequence. The levels are defined in table 1 and table 2.

The likelihood levels can be described as frequency values or with respect to how easy it is for a person to exploit a threat. For some threats it is easier to think of the likelihood in the form of frequency or a probability value. This may often be the case for threats related to availability, e.g. caused by problems in SW or HW. For other threats it is easier to think of

---

8 Staff from HN IKT is responsible for data extraction from the lab database.
likelihood when related to ease of misuse or mistake, or to motivation for performing a malicious action. – For each threat or unwanted incident we choose the most appropriate column or the column that is easiest to use in order to estimate the likelihood for the threat.

Table 1: Definition of likelihood levels

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Frequency</th>
<th>Ease of misuse Motivation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very high</td>
<td>Very often, occurs more often than every 10th connection, i.e. more frequently than 10% of the time/cases.</td>
<td>Can be done without any knowledge about the system; or without any additional equipment being used; or it can be performed by wrong or careless usage.</td>
</tr>
<tr>
<td>High</td>
<td>Quite often. Occurs between 1% and 10% of the time/cases.</td>
<td>Can be done with minor knowledge about the system; or without any additional equipment being used; or it can be performed by wrong or careless usage.</td>
</tr>
<tr>
<td>Moderate</td>
<td>May happen. Occurs between 0.1% and 1% of the time/cases.</td>
<td>Normal knowledge about the system is sufficient; or normally available equipment can be used; or it can be performed deliberately.</td>
</tr>
<tr>
<td>Low</td>
<td>Rare. Occurs less than 0.1% of the time/cases.</td>
<td>Detailed knowledge about the system is needed; or special equipment is needed; or it can only be performed deliberately and by help of internal personnel.</td>
</tr>
</tbody>
</table>

The consequence levels are described in terms of consequences for the patient (user) and consequences for the service or the service provider. In this case the service provider could be both the microbiology laboratory at UNN and/or the project owner (NST) and the Snow service. For each threat or unwanted incident we choose the most appropriate description to estimate the consequence level for the threat.

Table 2: Definition of consequence levels

<table>
<thead>
<tr>
<th>Consequence:</th>
<th>For the patient: No impact on health; or negligible economic loss which can be restored; or small reduction of reputation in the short run.</th>
<th>For the service provider: No violation of law; or negligible economic loss which can be restored; or small reduction of reputation in the short run.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Small</td>
<td>For the patient: No direct impact on health or a minor temporary impact; or economic loss which can be restored; or small reduction of reputation caused by revealing of less serious information (e.g. blood pressure level).</td>
<td>For the service provider: Offence, less serious violation of law which results in a warning or a command; or economic loss which can be restored; or reduction of reputation that may influence trust and respect.</td>
</tr>
<tr>
<td>Moderate</td>
<td>For the patient: Reduced health; or a large economic loss which cannot be restored; or serious loss of reputation caused by revealing of sensitive and offending information.</td>
<td>For the service provider: Violation of law which results in minor penalty or fine; or a large economic loss which cannot be restored; or serious loss of reputation that will influence trust and respect for a long time.</td>
</tr>
<tr>
<td>Severe</td>
<td>For the patient: Death or permanent reduction of health; or considerable economic loss which cannot be restored; or serious loss of reputation which permanently influences life, health, and economy.</td>
<td>For the service provider: Serious violation of law which results in penalty or fine; or considerable economic loss which cannot be restored; or serious loss of reputation which is devastating for trust and respect.</td>
</tr>
</tbody>
</table>
2.3.2 Acceptance criteria

We use accept criteria to define the acceptable risk level for the service. We cannot expect to achieve a risk level equal to zero. Thus we have to define which level of risk we consider as acceptable for the service we are analysing. The accept criteria should be based on the security requirements for the service.

The Norwegian Health Personnel Act (Helsepersonelloven) states in chapter 5 the obligation to maintain secrecy with respect to health information a person has been acquainted with in his or her duty as health personnel [10].

The following acceptance criteria have been proposed for the Snow service:

It is not acceptable that:

1. (C) – the likelihood is higher than low that unauthorised persons (i.e. anyone else than the patient, and those who have a treatment relation to the patient) get access to the patient’s personal health data (i.e. to sensitive data). This is regardless of why, where, and how it happens. (This means that in order to obtain unauthorised access to such data, detailed knowledge is needed about the technical system, or special equipment is needed, or it can only be performed by help of internal personnel.)

2. (A) – the likelihood is higher than moderate that the Snow service is unavailable for a period of time. (This corresponds to up to 24 minutes of a 40 hours’ work week, or that it happens not more than once for every 100 Snow accesses.)

3. (A) – the likelihood is higher than low that the Snow service causes reduced availability for the user’s local systems.

4. (I) – the likelihood is higher than low that information in the Snow system (request, results) is being modified. (I.e. more infrequent than once for every 1000 accesses to the Snow service.)

5. (Q) – the likelihood is higher than low that the information presented by the Snow client can be misinterpreted and cause wrong diagnosing. (I.e. more infrequent than once for every 1000 accesses to the Snow service.)

2.3.3 Risk levels

We have decided to use three distinct levels for risk: Low, Medium, and High. Our risk level definitions are presented in table 3.

The risk value for each threat is calculated as the product of consequence and likelihood values, illustrated in a two-dimensional matrix (figure 5). The shading of the matrix visualizes the different risk levels (the darker shading, the higher risk).

Based on the acceptance criteria, the risk level High is decided to be unacceptable. Any threat obtaining this risk level must be treated in order to have its risk reduced to an acceptable level. Threats with Low risk level are acceptable, and Medium risks have to be further looked into individually.

---

9 The letter in parenthesis refers to the security aspects: confidentiality (C), integrity (I), quality (Q), availability (A)
Table 3: Definition of risk levels

<table>
<thead>
<tr>
<th>Risk level:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>Acceptable risk. The service can be used with the identified threats, but the threats must be observed to discover changes that could increase the risk level.</td>
</tr>
<tr>
<td>Medium</td>
<td>The risk can be acceptable for this service, but for each threat the development of the risk must be monitored on a regular basis, with a following consideration whether necessary measures have to be implemented.</td>
</tr>
<tr>
<td>High</td>
<td>Not acceptable risk. Can not start using the service before risk reducing treatment has been implemented.</td>
</tr>
</tbody>
</table>

Figure 5: Risk matrix showing the defined risk levels

<table>
<thead>
<tr>
<th>Consequence:</th>
<th>Small</th>
<th>Moderate</th>
<th>Severe</th>
<th>Catastrophic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Likelihood:</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
</tr>
<tr>
<td>Moderate</td>
<td>Low</td>
<td>Medium</td>
<td>Medium</td>
<td>High</td>
</tr>
<tr>
<td>High</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>Very high</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
<td>High</td>
</tr>
</tbody>
</table>
3 Threat identification and analysis of risk

Approximately 40 threats and unwanted incidents have been identified. The threats are listed in the threat table in Annex A. For each possible threat we wanted to evaluate its impact or consequence and the likelihood that it would occur. Threats were given qualitative values for consequence and likelihood, according to definitions in tables 1 and 2.

Some of the threats have, however, been difficult to analyse with respect to consequence and in particular with respect to likelihood. It is difficult in the development phase to imagine the likelihood for possible unwanted incidents to happen when the system comes into operation. In particular, it is difficult to evaluate quality threats regarding misinterpretation and misunderstanding caused by presentation of results, before the service has been used. It is much easier to foresee consequences of such threats and unwanted incidents.

The risk value for each threat\(^\text{10}\) is defined as the product of consequence and likelihood values. To estimate the risk, the unique ID of the threat is written into the corresponding cell of the risk matrix, as shown in figure 6.

\begin{table}[h]
\centering
\begin{tabular}{|c|c|c|c|}
\hline
Consequence: & Small & Moderate & Severe & Catastrophic \\
\hline
Likelihood: & & & & \\
\hline
Low & c4.1, a1.1, a1.3, a1.4, a1.5, a1.6, a1.7, q5.2 & c1.1, c1.3, c1.4, c6.2, i1.1, i1.3, i1.4, i1.5, i3, i4.1, o1 & & \\
\hline
Moderate & & q4 & a2, i2, q1.2, q1.3, q5.1 & \\
\hline
High & c6.1 & & c3 & \\
\hline
Very high & & & q1.1 & \\
\hline
\end{tabular}
\caption{Risk matrix for the Snow service}
\end{table}

The placing of the identified threats in the risk matrix shows that approximately two third of the threats have been analysed to have a Low risk level. In most cases this low risk is caused the low likelihood estimated for these unwanted incidents.

Eleven of these threats with low risk have, however, been analysed to have Severe consequence. This is the case for several threats related to confidentiality (c1.1, c1.3, c1.4, c6.2) and integrity (i1.1, i1.3, i1.4, i1.5, i3, i4.1). The low likelihood for these threats is explained by the difficulty to access this (pseudonymous) information in the DMZ, and the

\(\text{10 The following 13 threats from the table in Annex A have not been given a risk value, for different reasons. These threats are therefore not included in the matrix:}\\
\begin{itemize}
\item c1.2, c2, a1.2, i1.2: External responsibility (HN IKT or NHN)
\item c4.2: NA for confidentiality
\item i4.2: NA for this (lab-)version of Snow
\item o2, o3: Open Source not considered a threat, refer to report [14]
\item c4.3, q2, q3: Not able to estimate likelihood.
\end{itemize}\)
assumed lack of motivation to do overcome this difficulty. But if the likelihood for these threats increases, their risk level will soon become unacceptably high.

The matrix also shows that while most of the confidentiality and integrity threats are analysed to have severe consequence, most of the threats to availability are analysed to have a lower consequence. A reason for this is that consequences of availability breaches in this case are mainly related to trust and reputation of the Snow service. (This could of course in some cases be devastating for Snow.) On the other hand, confidentiality breaches can be violation of law, and integrity and quality threats could, in worst cases, have consequences for patients’ health.

Some of the identified threats are discussed in more detail in the following subsections.

3.1 Threats with High risk level

In this analysis two threats have got an unacceptable high risk level.

c3 – Unauthorized persons get access to (pseudonymous) information which is also stored elsewhere, e.g. in other file systems, in other computers, on memory sticks, etc.

Data sets used during system development and testing, and data used for development of methods and models for detection and prediction of contagious diseases, are being stored several places outside the DMZ. This is pseudonym information extracted from the lab, but still sensitive. Without a well defined policy for secure handling of these data sets, the likelihood is considered high that unauthorised persons may get access to this information.

q1.1 – Missing analyses from the lab, because analysis with new codes are not exported from Safir.

New analysis codes are defined quite often. If there is no routine to update the extraction from Safir, analyses with these new codes will not be included in the extract from Safir to Snow and there could be many positive results that are not shown. In worst case a GP may give a wrong diagnosis based on poor quality information. In any case this would be bad reputation for the Snow service and lack of trust in the presented information.

3.2 Threats with Medium risk level

Six threats have got a medium risk level, and five of them are analysed to have Severe consequence. Even if threats with medium risk in principle could be acceptable, each of them should be investigated separately to see if they can cause additional problems.

In this case the conclusion is that none of these threats with medium risk are acceptable.

a2 – The Snow client causes reduced performance of other systems at the user (GP) side because the web reader takes all resources on the local PC.

With web sites containing more and more information, it is a general problem that the web reader also requires more of the local resources. The current version of Snow does not contain the huge amounts of data, and the likelihood is therefore set to moderate. But with a larger data set this is more likely to be a problem both for the users (GPs) and in particular for the reputation of Snow. In that case it is not an acceptable risk.

i2 – Information in the Report DB in the PO is modified by unauthorized persons through the Apache web server.

This could be done by SQL injection from a web client (not the Snow client). The Apache web server is placed in the NHN, i.e. in a more open environment than the DMZ. Everyone connected to NHN could access the web server. We therefore consider a moderate likelihood
for this to happen. According to the acceptance criteria, this risk is not acceptable. – MySQL is blocked for direct remote access, so the ReportDB cannot be directly modified.

q1.2 – Analyses from the lab not included, because Snow does not recognise the new analysis codes in the export files from Safir.

New analysis codes are defined quite often. If Snow does not detect and recognise these new codes, the consequence will be the same as for threat q1.1 in section 3.1 above. However, we consider this to be less likely than q1.1.

q1.3 – Analyses from the lab not included, because the lab has changed the result text (pos/neg) and Snow does not recognise the new text.

If this happens for the diagnoses included in Snow, the result may not be understood and therefore not included in the presentation. The consequence will be the same as for threat q1.1 in section 3.1 above. However, we consider this to be less likely than q1.1.

q5.1 – The PO produces old information because the LabServer does not receive new extracts from Safir after updates, or receives only parts of the extract from Safir.

This may happen if the update includes changes to the Safir DB. Safir is being updated quite often and the database queries are still being developed. The consequence of missing information is that the quality of the results published from PO is reduced as time goes by, it will be a mix of old and new information and this fact is not obvious to the user.

According to the acceptance criteria none of these three quality threats are acceptable.

q4 – Snow does not detect that a “new” analysis is really an earlier analysis that has been changed by the lab afterwards.

The consequence of this would be that the same analysis is counted twice, and the number of incidents will be wrong. The likelihood for this is analysed to be moderate (higher than low), but the consequence is considered to be moderate and therefore this risk could be accepted.

3.3 Threats with Low risk level

The remaining 20 threats have a low risk level. These are therefore acceptable risks, but one should occasionally keep an eye on them to see if they can cause new problems. Some of the risks could for instance change due to modifications of the service.

It is particularly important to observe the eleven low-risk-threats which have been analysed to have severe consequence. If the likelihood for these threats increases, their risk level will soon be unacceptably high. The low risk threats with severe consequence are therefore discussed specifically here.11

11 Low-risk-threats with consequence analysed to be lower than severe, are not discussed here.

q1.1 – Unauthorized persons get access to (pseudonymous) information in DMZ by access to the same network (physical access plus username and password).

The consequence is set to severe for the hospital if patient identities are revealed; that is a violation of law. We could say that in this case it is “less sensitive” information (diagnoses) so that the consequence for the patient is more moderate.

Based on assumptions about motivation and ease, we consider the likelihood to be low for externals to get access. – We do trust the personnel at HN IKT who have the same username
and password as the Snow developers. (They have root password to all servers at the hospital.)

c1.3, c1.4 – Unauthorized persons get access to (pseudonymous) information in DMZ, either by use of a fake/bogus agent that can retrieve information from the Snow DB (c1.3), or by modification of ‘Rules’ in ‘Import Manager’ (c1.4).

For both these threats we estimate the likelihood to be (very) low: In order to do this, the person must have access to LabServer in DMZ (see threat c1.1 above), and if a person has that access there are much simpler ways to obtain the same information.

c6.2 – Information being distributed from the PO and further out, is sensitive, i.e. it is not anonymous “enough” because of design weaknesses or programming errors in the LabAgent.

Such weaknesses or errors could imply that the aggregation is not performed correct and more detailed information than agreed on is distributed. There will, however, be many eyes on the presented result so this will be quickly discovered. Thus we estimate the likelihood to be low.

i1.1 – (Pseudonymous) information in DMZ is modified by unauthorised persons who get access to the same network (physical access plus username and password).

The consequence is set to severe both for the trust in the Snow service, and in worst case for the GP who sets the wrong diagnosis based on misleading information, and for the patient who is receiving the wrong treatment.

Based on assumptions about motivation and ease, we consider the likelihood to be low for externals to get access. – We do trust the personnel at HN IKT who have the same username and password as the Snow developers. (They have root password to all servers at the hospital.)

i1.3, i1.4 – (Pseudonymous) information in DMZ is modified by unauthorised persons, either by use of a fake/bogus agent (i1.3) or by modification of ‘Rules’ in ‘Import Manager’ (i1.4).

For both these threats we estimate the likelihood to be (very) low: In order to do this, the person must have access to LabServer in DMZ (see threat i1.1 above), and if a person has that access there are much simpler ways to modify the same information.

i1.5 – (Pseudonymous) information in the Snow DB in DMZ is modified by unauthorised persons who are able to send an SQL-command in a ‘Mission Spec’ via XMPP to LabServer.

To perform a sensible/meaningful modification of the Snow DB, it is necessary to have a certain knowledge of the DB structure, and the right certificate for the LabServer is needed. It is easier to perform a modification that corrupts or destroys the information in the Snow DB.

i3 – Information being transferred by XMPP from LabAgent to PO is modified by a ‘man-in-the-middle’ attack.

Based on motivation and ease, we consider the likelihood to be low. The implemented authentication method (SASL EXTERNAL) will also reduce the likelihood for this.

i4.1 – A fake/bogus agent is able to send (fake) data to the PO for publishing because of wrong configuration of the XMPP server.

In order for this to happen, the XMPP server must be configured to automatically create a new user if a client is unknown. In that case a malicious client can make the PO publish
“anything”, which could have severe consequence. Based on motivation and ease, however, we consider the likelihood to be low.

01 – **The Snow client is replaced by a fake/bogus application (e.g. a Trojan Horse) because an hacker attacks the PO web server.**

The Snow client is downloaded from the PO web server. If an “hacker” could replace the Snow client with his own malicious application (Trojan Horse) he could do all sorts of harm. But with the PO server in a restricted network like NHN we consider the likelihood for this to be low.

## 4 Conclusions and recommendations

### 4.1 Recommended risk treatment

There are basically four different approaches to handle a risk [3, 4]:

1. **Accept** the risk, in accordance with the organisation’s security policy. This approach is usually applied for the risks with an acceptable risk level. *It is worth remembering that accepting the risk does not mean accepting the unwanted incident indicated by the threat.*

2. **Reduce** the risk to an acceptable level. Since the risk is a product of likelihood and consequence, this means to reduce the likelihood, the consequence, or both. It is often difficult to reduce the consequence of a threat, so the focus should first of all be on reduction of the likelihood.

3. **Avoid** the risk, i.e. try not to be exposed to the risk, not do the things that could lead to the risk. (In our case this could mean not installing the Snow service.)

4. **Transfer** the risk to a third party (e.g. an insurance company)

In this analysis we will mainly stick to strategies 1 and 2 above and recommend security measures that can reduce risks to an acceptable level. Risk reduction should be subject to a cost/benefit analysis, and if cost effective, risks should be reduced based on the ALARP principle (As Low As Reasonable Possible).

The table in Annex B lists the threats with risk level **High** (from section 3.1) and **Medium** (from section 3.2) and the **Low** risk threats with severe consequence (from section 3.3), together with security measures proposed for treatment of these threats. Treatments of each of these threats are discussed in more detail in sub-sections 4.1.1 and 4.1.2.

Some of the other threats with Low risk level will also benefit from treatment proposed to threats with higher risk. Table 4 summarizes the proposed treatments for risk reduction, and lists the threats that would have their risk reduced by implementing these treatments.\(^\text{12}\)

Different treatment options are grouped under a few main headings:

- routines to be defined
- software improvement to be considered
- testing
- quality assurance.

Even if treatment options are grouped in this way, they are also depending on each other, and many of the threats will therefore appear with more than one type of treatment. – For instance; **routines** will be a good measure for handling changes in the Safir database (threats q1.2, q1.3), but improving the **software** to detect unknown data will also be a measure for

\(^{12}\) In this table the threats listed in Annex B are written in bold face print, while the rest of the threats with low risk are written in normal print.
reducing the risk level of these threats. Another example is threat i4.1 (the XMPP server allows other than the LabAgent to send data to PO for publishing): This can be helped both by quality assurance of the XMPP configuration and by improving the software to authenticate the sender.

Table 4: Proposed risk reduction treatment and affected threats

<table>
<thead>
<tr>
<th>Treatment; security measures</th>
<th>Affected threats</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policies, routines and procedures:</td>
<td></td>
</tr>
<tr>
<td>• when Safir is updated (test codes, results, etc.)</td>
<td>q1.1, q1.2, q1.3, q5.1</td>
</tr>
<tr>
<td>• handling of data sets from the lab</td>
<td>c3</td>
</tr>
<tr>
<td>• password policy</td>
<td>c1.1, i1.1</td>
</tr>
<tr>
<td>• support and maintenance</td>
<td>a1.3 – a1.7</td>
</tr>
<tr>
<td>Design decisions</td>
<td>c4.1, c6.1</td>
</tr>
<tr>
<td>Software improvement (e.g. input validation, authentication, etc.)</td>
<td>c4.1, i1.5, i2, i4.1, q1.2, q1.3, q4, q5.1, q5.2, o1</td>
</tr>
<tr>
<td>Test procedures</td>
<td>c6.2, a1.1, a1.4, a2, q5.1</td>
</tr>
<tr>
<td>Quality assurance (of configuration, results, etc)</td>
<td>c1.3, c1.4, c4.3, c6.2, a2, i1.3, i1.4, i4.1</td>
</tr>
</tbody>
</table>

4.1.1 Treatment of threats with High risk

This section discusses treatment of the threats from section 3.1.

c3 – Unauthorized persons get access to (pseudonymous) information which is also stored elsewhere, e.g. in other file systems, in other computers, on memory sticks, etc.

The first and most important treatment of this threat is to define policy and routines for handling such data from the Safir extract. The pseudonymous information is still sensitive and should not be available for unauthorised persons. The policy/routines should detail what this information consists of, where it is stored, how it is secured, and which persons are authorised to use the information. There should also be a routine for controlling the access to these data, e.g. a log function.

The data sets could for instance be stored on separate storage units which can be removed and locked in, and possibly encrypted. If the data sets stay on the harddisk of an online computer, they should be encrypted.

q1.1 – Missing analyses from the lab, because analysis with new codes are not exported from Safir.

The likelihood may not be quite as high as indicated in the analysis, but it is important to handle this risk anyway. The filter for extracting data from Safir needs manual update for every new code. The best solution will be to define a routine for giving the necessary information.

For instance: Every time a new code is included in Safir, the microbiology lab shall notify the Snow project, and the Snow project in turn shall notify HN IKT who actually will update the filter. In this way the Snow project is also informed about necessary updates needed for the Snow software (threat q1.2)
4.1.2 Treatment of threats with Medium risk

This section discusses treatment of the threats from section 3.2.

a2 – The Snow client causes reduced performance of other systems at the user (GP) side because the web reader takes all resources on the local PC.

One strategy is to compare the memory consumption of the Snow client with other web sites the user can access without problems. In addition, the memory consumption should be tested after all changes to the web client.

i2 – Information in the Report DB in the PO is modified by unauthorized persons through the Apache web server.

Input to the query should be validated, particularly with respect to possible SQL injection, by verifying that input does not contain any escape characters.

q1.2 – Analyses from the lab not included, because Snow does not recognise the new analysis codes in the export files from Safir.

The same routine as described for threat q1.1 (in section 4.1.1 above) will also be useful to prevent this threat (prospective). An alternative is to detect new/unknown codes by logging and then include them afterwards (in retrospect).

q1.3 – Analyses from the lab not included, because the lab has changed the result text (pos/neg) and Snow does not recognise the new text.

The treatment for this threat would be similar as for threat q1.2 above: If possible, have a routine for the lab to inform the Snow project about changes to the result definition, and/or alternatively, logging to detect new/unknown results.

q4 – Snow does not detect that a “new” analysis is really an earlier analysis that has been changed by the lab afterwards.

It must be possible for the Snow software (the Import Manager) to detect that a data record is an update to a previous result. Snow must then be able to update the old record instead of making a new one.

q5.1 – The PO produces old information because the LabServer does not receive new extracts from Safir after updates, or receives only parts of the extract from Safir.

See also threats q1.1, q1.2 and q1.3 above. As far as possible the Snow project should be informed about changes to Safir and the filter. It could also be useful to provide a standard test that HN IKT could run after modifications to the Safir extract.

It will be possible to detect that the PO receives only old information. Then the client could also be informed about this.

4.1.3 Treatment of severe threats with Low risk

This section discusses treatment of the threats from section 3.3. All these threats are in principle acceptable, but the proposed treatment should possibly be considered.

c1.1 – Unauthorized persons get access to (pseudonymous) information in DMZ by access to the same network (physical access plus username and password).

In general, a good password policy is the first level of protection. It should prevent unauthorised persons to log in to a computer on the same network.
Personnel at HN IKT have the same username and password as the Snow developers. They have root passwords to all servers at the hospital, so we have to trust them, i.e. accept the risk.

c1.3, c1.4 – Unauthorized persons get access to (pseudonymous) information in DMZ, either by use of a fake/bogus agent that can retrieve information from the Snow DB (c1.3), or by modification of ‘Rules’ in ‘Import Manager’ (c1.4).

Part of a treatment for this threat would be some quality checking of the “Rules”.

c6.2 – Information being distributed from the PO and further out, is sensitive, i.e. it is not anonymous “enough” because of design weaknesses or programming errors in the LabAgent.

To avoid programming errors in general there should be thorough testing of all subsystems. An automated “testline” should be planned that could be run before a new version is put into operation.

On the other hand, there will be many eyes on the presented result so if this happens it will be quickly discovered.

i1.1 – (Pseudonymous) information in DMZ is modified by unauthorised persons who get access to the same network (physical access plus username and password).

See threat c1.1 above.

i1.3, i1.4 – (Pseudonymous) information in DMZ is modified by unauthorised persons, either by use of a fake/bogus agent (i1.3) or by modification of ‘Rules’ in ‘Import Manager’ (i1.4).

See threats c1.3, c1.4 above.

i1.5 – (Pseudonymous) information in the Snow DB in DMZ is modified by unauthorised persons who are able to send an SQL-command in a ‘Mission Spec’ via XMPP to LabServer.

Input to the query should be validated (see threat i2 in section 4.1.2 above).

i3 – Information being transferred by XMPP from LabAgent to PO is modified by a ‘man-in-the-middle’ attack.

One way to handle this is to make sure that the publisher in PO only accepts messages from the LabAgent, possibly with the use of electronic signature.

i4.1 – A fake/bogus agent is able to send (fake) data to the PO for publishing because of wrong configuration of the XMPP server.

First of all, the configuration of the XMPP server should be checked so that it does not generate a new user if the client is unknown. As for threat i3 above, the PO should also verify that the message really comes from the LabAgent.

o1 – The Snow client is replaced by a fake/bogus application (e.g. a Trojan Horse) because an hacker attacks the PO web server.

Verify the authenticity of the Snow client by use of certificate and digital signature¹³.

---

¹³ .xap files can be digitally signed. That is normally done only when the Silverlight application is executed outside a web reader and has several privileges. With the introduction of Silverlight 4 and Visual Studio 2010 digital signing will be easier (Per Atle, 2010). See also http://blogs.infosupport.com/blogs/alexb/archive/2010/05/10/silverlight-4-digitally-signing-a-xap.aspx
4.2 Conclusions

In this second risk assessment of the Snow service we analysed in more detail the service that was first analysed in the fall of 2007 [13]. The current version of Snow gets its input data from hospital laboratory tests. The risk assessment therefore involved the microbiology laboratory at UNN.

The risk assessment identified two threats with an unacceptable High risk level (q1.1 and c3). Six threats were given a Medium risk level, and five of them (a2, i2, q1.2, q1.3, and q5.1) were evaluated to be unacceptable.

Among the threats with Low risk level we have focused especially on the eleven threats with severe consequence. The argument for this is that with an increased likelihood these threats will easily get an unacceptable risk level. A tendency, based on consequence, is that most of the confidentiality threats have severe consequence, while most of the availability threats have lower consequence. All integrity threats and many of the quality threats are also analysed to have severe consequence.

Measures for risk reduction have been proposed in section 4.1. Among these treatment options we want to mention the following from table 4:

- Definition of policies, routines and procedures for specific areas, like:
  ◦ how to handle changes to information in the Safir database at UNN (e.g. modified test codes and result descriptions)
  ◦ security of (pseudonymous) data from Safir which is being used in development and testing of Snow, and in connected research projects at NST
  ◦ supervision, support and maintenance of the operational Snow system
- Improvement of software with respect to input validation (queries, requests, authentication)
- Quality assurance and test procedures

It is the responsibility of the project management to follow up the implementation of the proposed treatment.
References


http://www.lovdata.no/all/lo-20000414-031.html

[9] Act on personal health data filing systems and the processing of personal health data [Personal Health Data Filing System Act] 
http://www.lovdata.no/all/lo-20010518-024.html

LOV-1999-07-02-64 – Lov 2. juli 1999 nr. 64 om helsepersonell m.v. (Helsepersonelloven). 
http://www.lovdata.no/all/lo-19990702-064.html


  programvare eller åpen kildekode i IKT-løsninger for helsesektoren. Nasjonalt senter
  http://www.telemed.no/informasjonssikkerhet-og-risiko-ved-bruk-av-fri-programvare-
  eller-aapen-kildekode-i-ikt-loesninger-for-helsesektoren.4524975-48869.html
### Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALARP</td>
<td>As Low As Reasonable Possible</td>
</tr>
<tr>
<td>DB</td>
<td>Database</td>
</tr>
<tr>
<td>DMZ</td>
<td>Demilitarized Zone</td>
</tr>
<tr>
<td>DoS</td>
<td>Denial of Service</td>
</tr>
<tr>
<td>EU</td>
<td>European Union</td>
</tr>
<tr>
<td>FTA</td>
<td>Fault Tree Analysis</td>
</tr>
<tr>
<td>GP</td>
<td>General Practitioner <em>(doctor)</em></td>
</tr>
<tr>
<td>HN IKT</td>
<td>Helse Nord IKT <em>(the Information Technology Organisation of Northern Norway Regional Health Authority)</em></td>
</tr>
<tr>
<td>HW</td>
<td>Hardware</td>
</tr>
<tr>
<td>ID</td>
<td>Identifier / Identification</td>
</tr>
<tr>
<td>ISO</td>
<td>International Standardisation Organisation</td>
</tr>
<tr>
<td>NA</td>
<td>Not applicable</td>
</tr>
<tr>
<td>NHN</td>
<td>Norwegian Health Net</td>
</tr>
<tr>
<td>NST</td>
<td>Norwegian Centre for Integrated Care and Telemedicine</td>
</tr>
<tr>
<td>PC</td>
<td>Personal Computer</td>
</tr>
<tr>
<td>PII</td>
<td>Personal Identifiable Information</td>
</tr>
<tr>
<td>PO</td>
<td>Post Office <em>(server in Snow)</em></td>
</tr>
<tr>
<td>SHA</td>
<td><em>hash algorithm for one-way encryption</em></td>
</tr>
<tr>
<td>SQL</td>
<td>Structured Query Language</td>
</tr>
<tr>
<td>SW</td>
<td>Software</td>
</tr>
<tr>
<td>TCP</td>
<td>Transmission Control Protocol</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</td>
</tr>
<tr>
<td>UNN</td>
<td>University Hospital of North Norway</td>
</tr>
<tr>
<td>XMPP</td>
<td>eXtensible Messaging and Presence Protocol</td>
</tr>
</tbody>
</table>
**Annex A Threat table**

The following table indicates likelihood, consequence and resulting risk level for each identified threat. (The values actually used in the analysis are indicated in **bold**.)

<table>
<thead>
<tr>
<th>ID</th>
<th>Threat / Unwanted incident</th>
<th>Cause</th>
<th>Likelihood</th>
<th>Consequence</th>
<th>Risk level</th>
<th>Comments and descriptions of implemented security measures</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Confidentiality: Sensitive information is revealed to unauthorised persons</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>c1.1</td>
<td>Access to (pseudonymous) information in DMZ, from SnowDB via LabServer, or from export-/import files (Safir extract files)</td>
<td>Unauthorised person gets access to the same network, i.e. physical access – plus username and password for network and server.</td>
<td>Low</td>
<td>Severe</td>
<td>Low</td>
<td>Person ID is made pseudonymous (hashed), but the information includes: Year of birth, sex, postal code for patient and GP, requisitioning GP (pseudonym), test time, recorded time, type of analysis, result of analysis. A combination of this information can reveal the identity of a person in small populations. - Must trust HN IKT, they have root password for all servers...</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- based on motivation and ease.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>But: Snow developers have the same username and password as HN IKT personnel.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- for UNN if patient identity is revealed,</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>- but Moderate for the patients? (Reputation).</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>In this case less serious info/disease.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>c1.2</td>
<td>Access from a terminal in HN IKT's server room at UNN, or theft of disk containing SnowDB from HN IKT's server room.</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>This is HN IKT's responsibility. It is in the same server room as the other servers for the hospital, and we expect this to be secure enough.</td>
</tr>
<tr>
<td>c1.3</td>
<td>Fake/bogus agent in DMZ which can retrieve information from SnowDB</td>
<td>Low</td>
<td>Low</td>
<td>Must have access to LabServer in DMZ to do this (see threats c1.1 and c1.2 above) – and if a person has such access, there are easier ways to retrieve data from the DB.</td>
<td>Low</td>
<td>Treatment: Quality checking of ‘Rules’</td>
</tr>
<tr>
<td>c1.4</td>
<td>Modify ‘Rules’ in ‘Import Manager’, e.g. by adding a rule for retrieving data from SnowDB</td>
<td>Low</td>
<td>Low</td>
<td>NA</td>
<td>NA</td>
<td></td>
</tr>
<tr>
<td>c2</td>
<td>Valid person-ID (unique birth nbr) can be recreated/guessed</td>
<td>The &quot;salt&quot; used for pseudonymisation in the filter between the internal Lab systems and DMZ, is revealed to unauthorised persons.</td>
<td>NA</td>
<td>Severe</td>
<td>NA</td>
<td>HN IKT is responsible for this part. Treatment: Routines?</td>
</tr>
<tr>
<td>ID</td>
<td>Threat / Unwanted incident</td>
<td>Cause</td>
<td>Likelihood</td>
<td>Consequence</td>
<td>Risk level</td>
<td>Comments and descriptions of implemented security measures</td>
</tr>
<tr>
<td>-----</td>
<td>--------------------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>------------</td>
<td>-------------</td>
<td>------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| c3  | Access to information (pseudonym) which also is stored in other file systems and in other computers and memory sticks and... | (Is used during system development and testing, and for research of models and methods for detection of diseases.)                                                                                      | High       | Severe      | High       | Treatment:  
- A separate server for these data sets, or:  
- Data encrypted on harddisk, or:  
- Separate storage units that can be removed and locked in, and possibly encrypted.  
→ Routines must be described.                                                                                                                                                               |
| c4  | External persons can retrieve data from SnowDB/LabServer through port 5269 (open for XMPP traffic over TCP) | External client sends a Mission Spec via XMPP to LabServer                                                                                                                                                                                                 | Low        | Moderate    | Low        | Treatment:  
- LabAgent must limit the time period  
(Later: Client authentication.)                                                                                                                                                                                                 |
| c4.1|                                                                                             | Need a valid agent certificate in LabServer and make a valid query                                                                                                                                     | Low        | NA          | NA         | Treatment:  
- for Confidentiality, (LabAgent fails, will not be able to process the request)  
Input to query must be validated.                                                                                                                                                               |
|     |                                                                                             | SQL injection in Mission Spec                                                                                                                                                                            | NA         | NA          | NA         |                                                                                                                                                                                                 |
| c4.2|                                                                                             | Exploit some other (unknown or hidden) functionality in "Openfire", e.g. the administrator interface                                                                                                  | ??         | ??          | ??         | Treatment:  
Functionality that is not being used should be deleted/blocked from the ‘Openfire’ installation, plug-ins that will not be used, shall not be installed.  
(The same is true for all sw…)                                                                                                                                                                |
| c4.3|                                                                                             | Openfire has not access to SnowDB                                                                                                           | ??         | ??          | ??         |                                                                                                                                                                                                 |
| c5  | Access to data during transfer to PO"publisher" (wiretapping)                              | Insufficient encryption                                                                                                                                                                                 | Low        | Null        | Null       | No reason to encrypt because the reports are free to be read by everyone  
(Encryption and decryption could be performed by the ‘Security Manager’ on both sides.)                                                                                                           |
<table>
<thead>
<tr>
<th>ID</th>
<th>Threat / Unwanted incident</th>
<th>Cause</th>
<th>Likelihood</th>
<th>Consequence</th>
<th>Risk level</th>
<th>Comments and descriptions of implemented security measures</th>
</tr>
</thead>
<tbody>
<tr>
<td>c6.1</td>
<td>Sensitive information is being distributed to PO – and further out to the clients. <em>(Information being distributed from the PO – and further out – is sensitive, i.e. not anonymous enough.)</em></td>
<td>In “county view” the number per month is given for each sex and age group. In “municipality view” only the total number per month is given. – If the number in a county is low, it is possible to deduct which municipality these persons belong to.</td>
<td>High</td>
<td>Small Lab defines this as &quot;less sensitive&quot; diagnoses, and the information is at least pseudonym</td>
<td>Low</td>
<td>Treatment: A solution could be to define a lower limit N for the total number in a county, below which the number per sex and age group shall not be shown.</td>
</tr>
<tr>
<td>c6.2</td>
<td></td>
<td>Programming errors in LabAgent – so that the aggregation is not performed correct and more detailed info than agreed on is distributed.</td>
<td>Low</td>
<td>Severe</td>
<td>Low</td>
<td>Treatment: - Thorough testing of all subsystems - In general: “Testline” before a new version is put into operation. (Must be planned/described.)</td>
</tr>
</tbody>
</table>

**Availability: Information is not available to authorised persons when needed/wanted**

<table>
<thead>
<tr>
<th>ID</th>
<th>(Information from) PO is not available</th>
<th>Web server not available</th>
<th>Low</th>
<th>Moderate</th>
<th>Low</th>
<th><em>(There are many sub-components in the PO)</em></th>
</tr>
</thead>
<tbody>
<tr>
<td>a1.2</td>
<td>For availability in the rest of the system – see under Quality <em>(→ old reports)</em></td>
<td>The health network is down</td>
<td>NA</td>
<td>- for Snow. GP and patients will manage without Snow ☺ ◆</td>
<td>NA</td>
<td>NHN responsibility...</td>
</tr>
<tr>
<td>a1.3</td>
<td></td>
<td>Power failure</td>
<td>Low</td>
<td></td>
<td>Low</td>
<td></td>
</tr>
<tr>
<td>a1.4</td>
<td></td>
<td>Server overload, due to too many simultaneous users</td>
<td>Low</td>
<td>All users are within Norwegian Healthcare network</td>
<td>Low</td>
<td></td>
</tr>
<tr>
<td>a1.5</td>
<td></td>
<td>ReportDB not available because SQL server has failed</td>
<td>Low</td>
<td></td>
<td>Low</td>
<td></td>
</tr>
<tr>
<td>a1.6</td>
<td></td>
<td>ReportDB not available because of disk crash</td>
<td>Low</td>
<td></td>
<td>Low</td>
<td></td>
</tr>
<tr>
<td>a1.7</td>
<td></td>
<td>DoS attack</td>
<td>Low</td>
<td></td>
<td>Low</td>
<td></td>
</tr>
<tr>
<td>a2</td>
<td>Snow client causes other systems at GP office to ‘hang’</td>
<td>The web reader takes all resources on local PC</td>
<td>Moderate</td>
<td>Severe - for Snow.</td>
<td>Medium</td>
<td>Is a general web reader problem, not only for Snow. Treatment: Compare Snow client’s memory consumption compared with often used sites, like VG. Testing after all changes to web client.</td>
</tr>
<tr>
<td>ID</td>
<td>Threat / Unwanted incident</td>
<td>Cause</td>
<td>Likelihood</td>
<td>Consequence</td>
<td>Risk level</td>
<td>Comments and descriptions of implemented security measures</td>
</tr>
<tr>
<td>----</td>
<td>----------------------------</td>
<td>-------</td>
<td>------------</td>
<td>-------------</td>
<td>------------</td>
<td>----------------------------------------------------------</td>
</tr>
<tr>
<td>i1.1</td>
<td>Information in SnowDB or in export-/import files (Safir extract files) in DMZ is modified by unauthorised persons.</td>
<td>Unauthorised person gets access to the same network, i.e. physical access – plus username and password for network and server.</td>
<td>Low</td>
<td>Severe</td>
<td>Low</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- based on motivation and ease. But: Snow developers have the same username and password as HN IKT personnel.</td>
<td>- for Snow/NST, - for patients, in worst case (could get wrong diagnosis), - for the GPs (giving the wrong diagnosis).</td>
<td></td>
<td>This is HN IKT's responsibility. It is in the same server room as the other servers for the hospital, and we expect this to be secure enough.</td>
</tr>
<tr>
<td>i1.2</td>
<td>Access from a terminal in HN IKT's server room at UNN.</td>
<td></td>
<td>- -</td>
<td></td>
<td>NA</td>
<td></td>
</tr>
<tr>
<td>i1.3</td>
<td>Fake/bogus agent in DMZ which can modify information in SnowDB</td>
<td>Low</td>
<td></td>
<td>Low</td>
<td>Low</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Must have access to LabServer in DMZ to do this (see threats i1.1 and i1.2 above) – and if a person has such access, there are easier ways to modify data in the DB.</td>
<td></td>
</tr>
<tr>
<td>i1.4</td>
<td>Modify 'Rules' in 'Import Manager', e.g. by adding a rule for modifying data in SnowDB</td>
<td>Low</td>
<td></td>
<td>Low</td>
<td></td>
<td></td>
</tr>
<tr>
<td>i1.5</td>
<td>External client sends a 'Mission Spec' with an SQL command via XMPP to LabServer</td>
<td>Low</td>
<td>- certificate is needed</td>
<td>Low</td>
<td>Treatment: Input to query must be validated.</td>
<td></td>
</tr>
<tr>
<td>i2</td>
<td>Information in ReportDB in PO is modified by unauthorised persons through the Apache web server</td>
<td>SQL injection from a web client (not the Snow client)</td>
<td>Moderate</td>
<td>Severe</td>
<td>Medium</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>- before treatment (a more open environment than the DMZ) - But Low after treatment</td>
<td></td>
<td>Treatment: Input to query must be validated. (Hibernate generates SQL code?) Everyone connected to the Norwegian Health Network have access. MySQL Server is blocked for direct remote access.</td>
<td></td>
</tr>
<tr>
<td>ID</td>
<td>Threat / Unwanted incident</td>
<td>Cause</td>
<td>Likelihood</td>
<td>Consequence</td>
<td>Risk level</td>
<td>Comments and descriptions of implemented security measures</td>
</tr>
<tr>
<td>---</td>
<td>-----------------------------</td>
<td>-------</td>
<td>------------</td>
<td>-------------</td>
<td>------------</td>
<td>----------------------------------------------------------</td>
</tr>
<tr>
<td>i3</td>
<td>Information during transfer by XMPP from LabAgent to PO/'publisher' is modified by unauthorised persons</td>
<td>Man-in-the-middle attack</td>
<td>Low</td>
<td>Severe - not easy to do</td>
<td>Low</td>
<td>(Potential) treatment: ‘Publisher’ must only accept messages from LabAgent (with el. signature)</td>
</tr>
<tr>
<td>i4.1</td>
<td>A fake/bogus agent sends data to PO/'publisher'</td>
<td>Wrong configuration: XMPP server automatically creates a new user if the client is unknown.</td>
<td>Low</td>
<td>Severe - can publish “anything”</td>
<td>Low</td>
<td>(Potential) treatment: Check the configuration of the XMPP server. Check that the sender is the LabAgent, ‘Publisher’ must only accept messages from LabAgent (with el. signature) Later, when external users (GPs) are allowed to specify reports, one has to check the source of the report and not overwrite reports generated by others (e.g. Snow internal reports)</td>
</tr>
<tr>
<td>i4.2</td>
<td>A legal Snow user (not the LabAgent) sends data to ‘Publisher’</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td></td>
</tr>
</tbody>
</table>

Data quality: Information to the client is misleading, insufficient or faulty

<p>| q1.1 | Missing analyses: Snow does not receive analyses from lab. | Lab analyses are not picked up because new analysis codes are not exported from Safir | Very High | Severe | High | Treatment: Have a regular/frequent routine to notify the Snow project – who notifies HN IKT to check the extract from Safir for possible updates. (Positive filter, i.e. manual routines needed to include new codes/diseases.) |
| q1.2 | Analyses with new codes are exported, but Snow does not recognise the new codes | Moderate | Low after treatment | Moderate | Medium | Treatment: Snow can log any new codes so that they can be included afterwards. |
| q1.3 | Lab changes the result text (pos/neg) so that Snow does not interpret the result ( \rightarrow ) not included in SnowDB | Moderate | Before treatment, for the diagnosis in this version of Snow | | Medium | E.g. change from ‘positive’ and ‘negative’ to ‘ps’ and ‘ng’... (A new text can turn up, which has not been allowed for.) Treatment: Also log unknown results. |</p>
<table>
<thead>
<tr>
<th>ID</th>
<th>Threat / Unwanted incident</th>
<th>Cause</th>
<th>Likelihood</th>
<th>Consequence</th>
<th>Risk level</th>
<th>Comments and descriptions of implemented security measures</th>
</tr>
</thead>
<tbody>
<tr>
<td>q2</td>
<td>Presentation of result is misinterpreted</td>
<td>Ex.1: Both influenza and common cold for the same patient. Shall this be counted as 1 or 2, and at which level? Ex.2: Wrong number (too many or too few positive or negative) if a new test is counted as a new case, but is really the same registered several times (as pos/neg).</td>
<td>??</td>
<td>Severe</td>
<td>??</td>
<td>Treatment: Need a good description of what is presented in each image. Must be considered carefully. The description must include the time period between tests to count it as a new case. This time period can vary for different tests.</td>
</tr>
<tr>
<td>q3</td>
<td>Presentation of result is wrong, gives a wrong picture of the situation.</td>
<td>• Not presented as described.</td>
<td>??</td>
<td>Moderate</td>
<td>??</td>
<td>Treatment: Depend on how good the information is explained.</td>
</tr>
<tr>
<td>q4</td>
<td>Result exported previously is changed by the lab afterwards</td>
<td>Moderate</td>
<td>Moderate</td>
<td>Moderate</td>
<td>Medium</td>
<td>Treatment: Old record to be updated. Must detect that it is the same record.</td>
</tr>
<tr>
<td>q5.1</td>
<td>PO receives old information (info not updated from lab)</td>
<td>• Lab server does not receive extracts from Safir after update (DB changed) Parts of the extract is missing after updates of Safir</td>
<td>Moderate</td>
<td>Severe</td>
<td>Medium</td>
<td>Treatment: It is possible to check that the PO only receives old information, - and the client can be informed about this HN IKT must inform about change in Safir extracts. The Snow project should provide a standard test that HN IKT could run after each modification.</td>
</tr>
<tr>
<td>q5.2</td>
<td>Lab server does not receive extracts because Safir has crashed</td>
<td>Low</td>
<td>Moderate</td>
<td>Low</td>
<td>Low</td>
<td></td>
</tr>
</tbody>
</table>

Side 29 av 33
<table>
<thead>
<tr>
<th>ID</th>
<th>Threat / Unwanted incident</th>
<th>Cause</th>
<th>Likelihood</th>
<th>Consequence</th>
<th>Risk level</th>
<th>Comments and descriptions of implemented security measures</th>
</tr>
</thead>
<tbody>
<tr>
<td>o1</td>
<td>The Snow client is replaced by a fake/bogus application – which can do all sorts of harm</td>
<td>An intruder hacks the PO web server (Trojan horse).</td>
<td>Low</td>
<td>Severe</td>
<td>Low</td>
<td>The Snow client can be downloaded from the PO web server. A ‘hacker’ could replace the Snow client by his own malicious web client.</td>
</tr>
<tr>
<td>o2</td>
<td>The Snow source code is available as Open Source</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>Refer to NST report [14] - It is the policies, routines and environment that is of importance. - Not “security by obscurity”. - Remember to change default passwords when using and publishing Open Source. - New users will need new certificates.</td>
</tr>
<tr>
<td>o3</td>
<td>Snow is using Open Source components</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td>NA</td>
<td></td>
</tr>
</tbody>
</table>


### Annex B Plan for implementation of security measures

Proposed measures for threats with risk levels *High* and *Medium* and threats with severe consequence are listed in the following table. This is a summary of the descriptions in section 4.1.

The table should be used in the follow-up of the risk treatment.

<table>
<thead>
<tr>
<th>ID</th>
<th>Threats, unwanted incidents</th>
<th>Security measures</th>
<th>Responsible</th>
<th>Deadline</th>
<th>Status</th>
</tr>
</thead>
</table>
| q1.1| Missing analyses from the lab, because analyses with new codes are not exported from Safir. | Define a routine for giving the necessary information needed to update the filter, for instance:  
   - the microbiology lab shall notify the Snow project  
   - the Snow project shall notify HN IKT  
   - HN IKT shall update the filter |             |          |        |
| c3  | Unauthorized persons get access to (pseudonymous) information which is also stored elsewhere, e.g. in other file systems, in other computers, on memory sticks, etc. | Define policy and routines for handling the data extracted from Safir.  
   The policy/routines should detail:  
   - what the information consists of  
   - where the information is stored  
   - how the information is secured  
   - who are authorised to use the information  
   - control of access to these data  
   A log function could be needed. |             |          |        |
| a2  | The Snow client causes reduced performance of other systems at the user (GP) side because the web reader takes all resources on the local PC. | Compare the memory consumption of the Snow client with other web sites the user can access without problems.  
   Test the memory consumption after all changes to the web client. |             |          |        |
<p>| i2  | Information in the ReportDB in the PO is modified by unauthorized persons through the Apache web server. | Validate input to the query, particularly with respect to SQL injection. |             |          |        |</p>
<table>
<thead>
<tr>
<th>ID</th>
<th>Threats, unwanted incidents</th>
<th>Security measures</th>
<th>Responsible</th>
<th>Deadline</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>q1.2</td>
<td>Analyses from the lab not included, because Snow does not recognise the new analysis codes in the export files from Safir.</td>
<td>Routine as described for threat q1.1 above, followed by the necessary updates to Snow. Alternative: detect new/unknown codes by logging and include them afterwards.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>q1.3</td>
<td>Analyses from the lab not included, because the lab has changed the result text (pos/neg) and Snow does not recognise the new text.</td>
<td>As for threat q1.2 above: Define a routine for the lab to inform the Snow project about changes to the result description. Alternatively, logging to detect new/unknown results.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| q4  | Snow does not detect that a “new” analysis is really an earlier analysis that has been changed by the lab afterwards.                                                                                                                                                                                                                             | Design, programming:  
  • Snow must detect that a data record is an update to a previous result.  
  • Snow must then update the old record instead of making a new one.                                                                                                                                                      |             |          |        |
| q5.1| The PO produces old information because the LabServer does not receive new extracts from Safir after updates, or receives only parts of the extract from Safir.                                                                                                                                                                          | As for threats q1.1, q1.2 and q1.3 above: Define a routine for the lab to inform the Snow project about changes to Safir and the filter. Provide a standard test for HN IKT to run after modifications to the Safir extract. Design/programming: Detect that the PO receives only old information and inform the client about this. |             |          |        |
| c1.1| Unauthorized persons get access to (pseudonymous) information in DMZ by access to the same network (physical access plus username and password).                                                                                                                                                                                                 | Good password policy.  
  (And accept the risk...)                                                                                                                                                                                                                                                                                                                      |             |          |        |
<p>| i1.1| (Pseudonymous) information in DMZ is modified by unauthorised persons who get access to the same network (physical access plus username and password).                                                                                                                                                                                                 |                                                                                                                                                                                                                                                                                                                                               |             |          |        |</p>
<table>
<thead>
<tr>
<th>ID</th>
<th>Threats, unwanted incidents</th>
<th>Security measures</th>
<th>Responsible</th>
<th>Deadline</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>c1.3</td>
<td>Unauthorized persons get access to (pseudonymous) information in DMZ, either by use of a fake/bogus agent that can retrieve information from the Snow DB, or by modification of ‘Rules’ in ‘Import Manager’.</td>
<td>Quality checking of the “Rules”.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>c1.4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>i1.3</td>
<td>(Pseudonymous) information in DMZ is modified by unauthorised persons, either by use of a fake/bogus agent or by modification of ‘Rules’ in ‘Import Manager’.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>i1.4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>c6.2</td>
<td>Information being distributed from the PO and further out, is sensitive, i.e. it is not anonymous “enough” because of design weaknesses or programming errors in the LabAgent.</td>
<td>Thorough testing of all subsystems. An automated “testline” to be run before a new version is put into operation. Quality checking of the result/reports.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>i1.5</td>
<td>(Pseudonymous) information in the Snow DB in DMZ is modified by unauthorised persons who are able to send an SQL-command in a ‘Mission Spec’ via XMPP to LabServer.</td>
<td>Validation of input to query (see threat i2 above).</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>i3</td>
<td>Information being transferred by XMPP from LabAgent to PO is modified by a ‘man-in-the-middle’ attack.</td>
<td>PO shall only accept messages from the LabAgent, e.g. by use of digital signature.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>i4.1</td>
<td>A fake/bogus agent is able to send (fake) data to the PO for publishing because of wrong configuration of the XMPP server.</td>
<td>Check the configuration of the XMPP server. As for threat i3 above, the PO shall only accept messages from the LabAgent.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>o1</td>
<td>The Snow client is replaced by a fake application (e.g. a Trojan Horse) because a hacker attacks the PO web server.</td>
<td>Verify the authenticity of the Snow client (certificate and digital signature).</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Snow systemet
for legekontor og laboratorier

Driftsrutiner og kontroll

Versjon: 1.1

Forfattere:
Lars Ilebrekke,
Per Atle Bakkevoll,
Erlend Bønes,
Gustav Bellika,
Torje Henriksen
Revisjonshistorik:

<table>
<thead>
<tr>
<th>Nr</th>
<th>Detaljer</th>
<th>Hvem</th>
<th>Dato</th>
</tr>
</thead>
<tbody>
<tr>
<td>0.1</td>
<td>Første versjon opprettet.</td>
<td>Lars I</td>
<td>13.09.2011</td>
</tr>
<tr>
<td>0.2</td>
<td>Tilpasset etter sirkulering og diskusjon av tiltak</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.0</td>
<td>Etter diskusjon og revidering i teamet.</td>
<td></td>
<td>03.01.2012</td>
</tr>
<tr>
<td>1.1</td>
<td>NST ved UNN ansvarlig.</td>
<td>Gustav/Per Bruvoll</td>
<td>16.01.2012</td>
</tr>
</tbody>
</table>
Innhold
1 Innledning ................................................................................................................. 4
2 Krav for å sikre drift på legekontor ........................................................................... 5
  2.1 Ytelseskrav ........................................................................................................... 5
  2.2 Konfigurasjonskrav for datakildetjener ................................................................. 6
  2.3 Konfigurasjonskrav for arbeidsstasjoner ............................................................... 6
  2.4 Endring eller tilpasning av programvare ............................................................... 6
  2.5 Annet ..................................................................................................................... 6
3 Rutiner og krav til Snow systemet ........................................................................... 7
  3.1 Koordineringstjeneren (PO) ................................................................................. 7
    3.1.1 Oppetid ............................................................................................................ 7
    3.1.2 Informasjon om vedlikehold og eventuelle feil ............................................... 7
    3.1.3 Nødroutine ..................................................................................................... 7
    3.1.4 Meldingsovervåkning ...................................................................................... 7
  3.2 Oppdatering av datakildetjenere .......................................................................... 8
    3.2.1 Konfigurasjon .................................................................................................. 8
    3.2.2 Kontroll av ny Snow programvare ................................................................. 8
  3.3 Ivaretakelse av datakvalitet fra Mikrobiologilaboratoriet ved UNN .................... 10
Signering ..................................................................................................................... 11
Vedlegg ....................................................................................................................... 12
  Automatisk oppdatering av Snow programvare ....................................................... 12
  Sikkerhetskontroll av Snow programvare ............................................................... 13
1 Innledning

Nasjonalt senter for Samhandling og Telemedisin (NST) ved Universitetssykehuset i Nord-Norge er ansvarlig og eier av Snow systemet. Daglig drift, utvikling og oppfølging foretas av Snow teamet (prosjektmedarbeidere i Snow prosjektet er knyttet til NST, Tromsø Telemedicine Laboratory (TTL) og Universitetet i Tromsø).

Dette dokumentet beskriver håndtering av de tiltakene som ble lagt til grunn etter risikoanalysen av Snow legekontorløsning. Tiltak knyttet til drift av systemet, overvåkning av meldinger og rutiner for å ivareta tjeneste-kvalitet er omfattet i dokumentet. Figuren under gir en oversikt over Snow systemet med et forenklet scenario der legekontor X og legekontor Y er tilknyttet Snow.

Snow teamet har i dag en koordineringstjener\(^1\) (PO) i helsenettet. Denne tilbyr en nett klient som er tilgjengelig på [http://snow.nhn.no](http://snow.nhn.no). Den gir en geografisk oversikt over smittedata basert på data fra mikrobiologilaboratoriet ved UNN, og etter hvert symptomer basert på data fra tilknyttede legekontorer. Hver node (koordineringstjener eller datakildetjener) kjører en XMPP (Extensible Messaging and Presence Protocol) tjenere for utveksling av meldinger. Laboratoriet ved UNN er tilkoblet Snow systemet på samme måte som vist for legekontor X og legekontor Y.

På hver datakildetjener\(^2\) ligger det et database med navn SnowGpDb. Dette er Snow systemet sin lokale knukspsdatabase. Den bygges opp lokalt ved hjelp av kontrollerte uttrekk fra journalsystemet.

Videre i dette dokumentet deler vi inn i et kapittel om krav til datakildeleverandør (legekontor og laboratorier) og et kapittel om krav til Snow systemet generelt (Snow teamet er ansvarlig).

**NB: Før en ny datakildeleverandør kan tilknyttes må kravene i neste kapittel være gjennomlest og tatt til etterretning.**

\(^1\) Koordineringstjener er et annet navn for Post Office (PO) begrepet i Snow arkitekturan.

\(^2\) Datakildetjener er et annet navn for General Practice (GP) begrepet i Snow arkitekturan.

© Snow team 2012
2 Krav for å sikre drift på legekontor

Dette kapittelet beskriver kravene til omgivelsene en Snow datakildetjener kan installeres i. For å sikre forsvarlig drift av Snow systemet må noen krav være tilfredsstillt. Dersom legekontoret ikke har tilgjengelig en tjener som tilfredsstiller minimumskravene må Snow teamet kontaktes for hvordan dette kan håndteres. Kravene vil være like uavhengig av om tjeneren allerede er installert på kontoret, eller om en ny må anskaffes.

Snow systemet benytter fri programvare.

2.1 Ytelseskrav

En datakildetjener i Snow systemet må kjøre fem moduler der en av dem er databaseprogramvaren (MySQL Community Server). De fire modulene som er utviklet eller tilpasset av Snow teamet er:

- **Jive Openfire XMPP server.** Denne inkluderer komponenter utviklet av Snow teamet for blant annet koordinering av datainnsamling.

- **Praksismonitor** – denne modulen settes opp med planlagte uttrekk fra legekontorets journalsystem og overfører en begrenset mengde data til den lokale Snow kunnskapsbasen (MySQL). Modulen støtter eksport fra Compugroup Medical WinMed classic og Vision.

- **Snow-agenter** – denne modulen inneholder legekontoragenten (GpAgent) som leser den lokale kunnskapsdatabasen og aggererer dataene til anonyme rapporter som overleveres til koordineringstjeneren i helsenettet.

- **Oppdateringstjenesten** – denne kontakter Snow systemet sentralt for å spørre om eventuelle endringer på de ulike Snow modulene. Dersom det foreligger endringer vil oppdatering bli utført. Mer detaljert informasjon foreligger i vedlegget "Automatisk oppdatering av Snow programvare".

Systemet settes opp slik at uttrekk av data skjer utenom arbeidstid. Det samme gjelder også for koordineringstjenerens innsamling av aggregerte rapporter og eventuelle oppdateringer av programvare. Det er kun meldingstjeneren (Openfire) og databasetjeneren (MySQL) som kjører kontinuerlig.

Det må legges til at minnebruk er viktigere enn prosessorkraft da en datakildetjener i Snow systemet ikke har strenge tidskrav for overlevering av rapporter. Minnekravene listes i tabellen under:

<table>
<thead>
<tr>
<th>Modul</th>
<th>Minimum minnekrav</th>
</tr>
</thead>
<tbody>
<tr>
<td>MySQL community server</td>
<td>128 MB</td>
</tr>
<tr>
<td>Praksismonitor</td>
<td>128 MB</td>
</tr>
<tr>
<td>Snow-agenter</td>
<td>128 MB</td>
</tr>
<tr>
<td>Oppdateringstjenesten</td>
<td>128 MB</td>
</tr>
<tr>
<td>Jive Openfire XMPP server</td>
<td><strong>256 MB</strong></td>
</tr>
</tbody>
</table>

På bakgrunn av hvordan systemet settes opp forventer vi ikke at minnebruk vil overstige 512 MB.
2.2 Konfigurasjonskrav for datakildetjener

Følgende krav gjelder for datakildetjeneren:
- For datakildetjeneren støttes følgende operativsystemer:
  - Microsoft Windows Server 2003 og 2003 R2
  - Microsoft Windows Server 2008 og 2008 R2
  - Microsoft Windows XP (32 bit)
  - Microsoft Windows Vista (32 og 64 bit)
  - Microsoft Windows 7 (32 og 64 bit)
- Operativsystemoppdateringer må installeres automatisk eller følge en streng oppdateringsrutine som ellers følges på legekontoret.
- Tjeneren må ha installert Anti-virus programvare som oppdateres jevnt.
- Tjeneren må være fysisk sikret slik at kun ansatte ved kontoret eller autorisert personell har tilgang.
- Tjeneren må kunne nåes på port 5269 fra koordineringstjeneren (PO) i helsenettet.\(^4\)
- Tjeneren må kunne nå koordineringstjeneren via http på port 80 (eventuelt via proxy) for oppdateringstjenesten.
- Tjeneren må kunne nå journaldatabaseen slik at uttrekk kan utføres.

2.3 Konfigurasjonskrav for arbeidsstasjoner

- For arbeidsstasjoner som skal bruke Snow-systemets nettsideklient, kreves operativsystem og nettleser med støtte for Silverlight 4, samt Silverlight plug-in. For eksempel:
  - Windows XP med Internet Explorer eller Firefox
  - Windows 7 med Internet Explorer eller Firefox
  - Windows Vista med Internet Explorer eller Firefox
  - Mac OS X med Safari
- Det anbefales en skjermoppløsning på minst 1024x768 piksler.

2.4 Endring eller tilpasning av programvare

Snow prosjektet kan ikke ta ansvær for eventuelle tilpasninger som blir gjort av legekontoret utenom de retningslinjer som er lagt. Snow prosjektet har ved installasjon og oppdateringer kontroll av konfigurasjon og moduler, men det er meget vanskelig for prosjektet å låse for at lokale brukere med riktig tilgang gjør endringer.

Eksempelvis er Openfire utvidbart (ved hjelp av tilgjengelige plugins) og relativt enkel å tilpasse med endring av konfigurasjonsparametere. Denne muligheten må ikke benyttes da det kan få konsekvenser for hvordan Snow systemet fungerer. For å kontrollere dette bedre har vi deaktivert det medfølgende brukergrensesnittet for slike tilpasninger.

2.5 Annet

Snow prosjektet vil senere tilby XMPP-klient programvare som åper opp muligheter for chat kommunikasjon mellom leger. I den forbindelse anbefales aktivering av kopiperre fra journalsystem dersom dette er tilgjengelig.

---
\(^{1}\) Ikke starter-edition
\(^{4}\) En del av dette gjøres ved å formelt be om at Norsk Helsenett SF sørger for denne tilgangen.

Side 6 of 13

© Snow team 2012
3 Rutiner og krav til Snow systemet
Dette kapitlet beskriver hva vi (Snow teamet) gjør for å sikre drift og vedlikehold av Snow.

3.1 Koordineringstjeneren (PO)
Det er hovedsakelig to grunner til at koordineringstjeneren er sentral i hvordan Snow systemet er satt opp. Den ene er at den er ansvarlig for koordinering av datainnsamling fra datakildetjenere, og den andre fordi den tilbyr Snow klienten tilgang til aggregerte rapporter innanset fra alle tilgjengelige datakilder.

3.1.1 Oppetid
Ved siden av at tjeneren (Fujitsu Primergy TX 100) lover hoy grad av oppetid vil Snow teamet alltid ha en reservetjener klar til bruk. Denne oppdateres fortøende på samme måte som hovedtjeneren. I tillegg blir det tatt backup av databasen en gang per døgn til en USB minnebrikke slik at reserveløsningen raskest mulig også har oppdaterte data frem til neste planlagte innsamling av aggregerte kildedata.

3.1.2 Informasjon om vedlikehold og eventuelle feil
Det blir opprettet en informasjonsside på NST sine netsider som beskriver når det vil være planlagt vedlikehold som gjør at Snow klienten ikke vil være tilgjengelig. En link til siden blir lagt ut på ”http://www.telemed.no/snow”. Det skal også rapporteres om det er tilfeller der koordineringstjeneren har vært nede utenom planlagt vedlikehold.

3.1.3 Nødrutine
Når systemet er utilgjengelig på grunn av ikke planlagte avvik over lengre tid skal alle i intervænsjonssrappen informeres. Vi regner ikke med at legekontor som tilhører kontrollgruppen har samme informasjonsbehov selv om de også har Snow installert.

3.1.4 Meldingsovervåkning

\(^5\) LTS – Long Term Support
Side 7 of 13

Dato 16.01.2012

© Snow team 2012
3.2 **Oppdatering av datakildetjenere**

Denne seksjonen beskriver oppdatering av datakildetjenere med fokus på hvordan konfigurasjonen av modulene ivaretas og hvordan datakilden verifiserer at det er korrekt programvare som er overført.

3.2.1 **Konfigurasjon**

I XMPP-tjeneren (en tilpasset versjon av Jive Openfire XMPP server) er det en systemklasse som setter de viktigste konfigurasjonsverdiene. I tillegg gjøres oppdateringer slik at konfigurasjonsfilen aldri blir skrevet over. Det vil fortsatt være mulig å gjøre endringer for lokale administratorer, men dette må koordineres med Snow teamet.

Operativsystemoppdateringer på tjenere som står utenfor Snow teamets kontroll (datakildetjenere) må utføres, men er ikke Snow teamets ansvar. Det er heller ikke Snow teamet sitt ansvar å påse at brannmurene på disse tjenere fortsetter å være riktige etter en oppdatering, men det er vesentlig at port 5269 (XMPP) er åpen mot helsenettet. I nettverket er dette også under kontroll av Norsk helsenett som må få skriftlig melding om åpning av brannmure mot Snow koordineringstjener i helsenettet.

3.2.2 **Kontroll av ny Snow programvare**

Denne seksjonen beskriver hvordan programoppdateringer signeres og verifiseres etter nedlasting. En mer detaljert beskrivelse er lagt ved i vedlegg "Snows oppdateringstjeneste omfatter følgende programvare:

- XMPP-tjener med Snow protokoll tilpasninger
- Praksismonitor
- Snow-agenter

I tillegg må MySQL databasesystem og Java være installert på maskinen. Disse omfattes ikke av oppdateringstjenesten.

For å forenkle installasjon av nye versjoner av programvaren bruker Snow automatisk oppdatering. Dette gjør at nye versjoner av programvaren lastes ned og installeres uten at brukerne trenger å tenke på dette.

På legekontoret kjører det en oppdateringstjeneste som en gang i døgnet sjekker mot en sentral oppdateringstjener om det er kommet oppdateringer til programvaren. I så fall lastes en oppdateringspakke ned til legekontoret. Etter at oppdateringspakken er lastet ned utføres det en sikkerhetssjekk av pakken før den eventuelt installeres.

Den sentrale oppdateringstjeneren inneholder to nettjenester, en for å sjekke om det foreligger oppdateringer, og en for å laste ned denne oppdateringen. Alle filer som inngår i oppdateringen er pakket inn i en zip-fil, dvs et filarkiv. For å sikre at oppdateringen inneholder autentisk kode blir zip-filen digitalt signert av Snow teamet før den blir lagt ut på oppdateringstjeneren. Denne signaturen må verifiseres før installasjonen på legekontoret kan fullføres.

Tidspunktet for automatisk oppdateringssjekk må ikke kollidere med tidspunktet for når backup kjøres internt på legekontoret. Nøyaktig tidspunkt må derfor avklares med hvert enkelt legekontor.

Side 8 of 13

© Snow team 2012

Dato 16.01.2012
Stegene i oppdateringsprosessen er som følger:

1. For hver installerte Snow programvare kaller oppdateringsklienten på legekontoret en nettjeneste på den sentrale oppdateringstjeneren for å sjekke om det finnes en oppdatering.
2. Dersom oppdatering finnes kalles en ny nettjeneste som returnerer en digitalt signert zip-fil som inneholder oppdateringspakken.
4. Dersom signaturen godkjennes pakkes alle enkelttfiler i oppdateringspakken ut av zip-filen.
5. Oppdateringsklienten starter et oppdateringsskript som først stopper det aktuelle programmet dersom det allerede kjører. Deretter kopieres filene i oppdateringspakken til riktig sted. Til slutt startes det oppdaterte programmet på nytt.

Sikkerhetskontroll av Snow programvare”. Prosedyren er som følger:

- En kryptografisk signeringsnøkkel er lagret på en USB-brikke som er fysisk sikret slik at uvedkommende ikke får tilgang til den.
- Nøkkelen er beskyttet med et passord som må oppgis for å låse den opp slik at den kan brukes til signering.
- Signeringen av koden skjer på en laptop som ikke er på nett og som oppbevares fysisk sikret. Den ferdig signerte koden kopieres til en USB-brikke slik at den kan overføres videre til oppdateringsserveren.
- Snow programvaren på legekontoret sjekker daglig om det er kommet nye oppdateringer. Disse lastes i tilfelle ned. Signeringen verifiseres, dersom denne mislykkes forkastes oppdateringen.

**Signeringstjener/laptop**


**Oppdateringstjener**

*Her er den signerte koden lagret, klar for nedlasting til legekontor*

**Legekontor**

*Snow-programvaren som kjører på legekontoret sjekker daglig om det er kommet nye oppdateringer. I så fall lastes nye zip-fil ned. Signeringen verifiseres og dersom den er ok, installeres oppdateringen. Hvis verifiseringen av signatur mislykkes forkastes oppdateringen.*
3.3 Ivaretakelse av datakvalitet fra Mikrobiologilaboratoriet ved UNN

Denne seksjonen beskriver rutiner på en del av systemet som ikke påvirker legekontor som datakildeleverandører. Manglende kvalitet på dette vil i første omgang påvirke innholdet som presenteres i nett klienten som tilbys på koordineringstjeneren (Post Office). Altså kan brukere få et galt bilde av prøveanalysesituasjonen på laboratoriet, uten at dette påvirker den tekniske overføringen fra legekontor til tjeneren i helsenettet.

Videre beskriver vi rutiner for kontroll av at nye analysekoder som blir tatt i bruk også blir lagt til i datauttrekket til Snow systemet dersom analysen faller inn under Snow systemets symptomgrupper. Figuren under gir en oversikt over systemet og hvordan IKT koordinatoren ved Avdeling for Mikrobiologi og Smittevern (AMS) kan tilpasse filteret som bestemmer hva som trekkes ut av databasen og overføres til Snow Systemet.

Avtalen mellom laboratoriet og Snow prosjektet legger til grunn at rapporteringen fra laboratoriet skal skje en gang per måned. Dette gjelder uavhengig av om det er gjort endringer på filteret eller ikke. I følge opplysinger vi har fått vil et ta noe tid fra en analysekode legges inn i laboratoriesystemet før den blir tatt i bruk på reelle prøver.

Med denne rutinen etablert vil Snow systemet med rimelig sikkerhet være oppdatert med det som er av tilgjengelig prøvesvar knyttet til de symptomgruppene som støttes.
Signering

Ved gjennomføring av risikoanalysen 16. mai 2011 kom analyseleder (Gustav Bellika) frem til enkelte tiltak for å redusere risiko for de involverte legekontorene i studien. Tiltakene består i å etablere driftsrutiner, opplæringsopplegg og utvikling av ny programvare i Snow systemet. Dette arbeidet er nå utført.

Per Bruvold
Sikkerhetssjef IKT/Personvernombud
UNN

den 16.1.12

Bjørn Engum
Senterleder
NST

den 16.1.12

© Snow team 2012
Vedlegg

Automatisk oppdatering av Snow programvare

Snows oppdateringstjeneste omfatter følgende programvare:

- XMPP-tjener med Snow protokoll tilpasninger
- Praksismonitor
- Snow-agenter

I tillegg må MySQL databasesystem og Java være installert på maskinen. Disse omfattes ikke av oppdateringstjenesten.

For å forenkle installasjon av nye versjoner av programvaren bruker Snow automatisk oppdatering. Dette gjør at nye versjoner av programvaren lastes ned og installeres uten at brukerne trenger å tenke på dette.

På legekontoret kjøres det en oppdateringstjeneste som en gang i døgnet sjekker mot en sentral oppdateringstjener om det er kommet oppdateringer til programvaren. I så fall lastes en oppdateringspakke ned til legekontoret. Etter at oppdateringspakken er lastet ned utføres det en sikkerhetssjekk av pakken før den eventuelt installeres.

Den sentrale oppdateringstjeneren inneholder to nettjenester, en for å sjekke om det foreligger oppdateringer, og en for å laste ned denne oppdateringen. Alle filer som inngår i oppdateringen er pakket inn i en zip-fil, dvs et filarkiv. For å sikre at oppdateringen inneholder autentisk kode blir zip-filen digitalt signert av Snow teamet før den blir lagt ut på oppdateringstjeneren. Denne signaturen må verifiseres før installasjonen på legekontoret kan fullføres.

Tidspunktet for automatisk oppdateringssjekk må ikke kollidere med tidspunkt for når backup kjøres internt på legekontoret. Nøyaktig tidspunkt må derfor avklares med hvert enkelt legekontor.

Stegene i oppdateringsprosessen er som følger:

6. For hver installerte Snow programvare kaller oppdateringsklienten på legekontoret en nettjeneste på den sentrale oppdateringstjeneren for å sjekke om det finnes en oppdatering.
8. Signaturen på oppdateringspakken verifiseres.

Side 12 of 13

Dato 16.01.2012

© Snow team 2012
Sikkerhetskontroll av Snow programvare

Ved nedlasting av programvare fra en annen tjener (utenfor det lokale nettverket) må vi være sikre på at programvaren er autentisk, det vil si at den faktisk kommer fra Snow og at ingen utenforstående har tuklet med den. For å sikre dette blir Snow programvaren utstyrt med en digital signatur. Denne signaturen må godkjennes på legekontorsiden før oppdateringene kan installeres.


Dersom zip-filen har blitt manipulert av utenforstående, det vil si nye filer har blitt lagt til eller enkeltfiler er byttet ut med en annen fil med samme navn, så vil dette bli oppdaget ved verifisering av signaturen og zip-filen blir forkastet.

Ved vellykket verifisering er integriteten til programvaren bekrøftet. Enkeltfilene i zip-filen blir pakket ut og et installasjonsskript blir kjørt for å fullføre oppdateringen.

---

⁶ Jarsigner verktøyet er en del av Java utviklingspakken fra Oracle.

© Snow team 2012

Dato 16.01.2012
Ledelsesrapport

Analyse: **Snow – symptombasert sykdomsovervåking**

**Status:**

Det finnes trusler som anses å kunne føre til høy skadekostnad om de inntreffer og det tilrås derfor at de mangler som er årsaken til disse truslene, tas tak i relativt omgående og med høy prioritet.

Scenariene ble prioritert av verktøyet og arbeidsgruppen på følgende måte etter størrelsen på risikokostnadene:

<table>
<thead>
<tr>
<th>Tittel</th>
<th>Frekvens</th>
<th>Skadekostnad</th>
<th>Risikokostnad</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feilaktig data presenteres</td>
<td>Høy</td>
<td>Høy</td>
<td>Moderat</td>
</tr>
<tr>
<td>Dårlig kvalitet på helsehjelp</td>
<td>Moderat</td>
<td>Høy</td>
<td>Moderat</td>
</tr>
<tr>
<td>Pasientdata slettes</td>
<td>Moderat</td>
<td>Høy</td>
<td>Moderat</td>
</tr>
<tr>
<td>PO-server blir compromittert</td>
<td>Moderat</td>
<td>Høy</td>
<td>Moderat</td>
</tr>
<tr>
<td>Pasientinfo blir tilgjengelig for uvedkommende</td>
<td>Lav</td>
<td>Høy</td>
<td>Moderat</td>
</tr>
</tbody>
</table>

Figure 1. X akse – frekvens, Y akse - skadekostnad

N5: Feilaktig data presenteres
N4: PO-server blir compromittert
N3: Pasientdata slettes
N2: Dårlig kvalitet på helsehjelp
N1: Pasientinfo blir tilgjengelig for uvedkommende
Risikokostnaden er den forventede årlige kostnaden som kan ramme virksomheten hvis ikke tiltak iverkesettes for å eliminere eller redusere de mangler som gjør scenariet mulig.

**Anbefalinger:**
Arbeidsgruppen fant fram til 20 tiltak for å redusere risiko hvorav 15 ble valgt ut til handlingsplanen. Disse ble prioritet av verktøyet etter økonomiske forutsetninger basert på den såkalte nettoeffektiviteten for hvert tiltak.

Nettoeffektiviteten tilsvarer den økonomiske nytte tiltaket virker på alle mangler det virker mot – gjennom å eliminere eller redusere mangelkostnaden – fratrukket tiltakets kostnad. Arbeidsgruppen gjorde senere sin egen prioritering av tiltakene etter en skala på (5) prioriteter som følger:

Prioritet 1 Svært viktig tiltak. Skal/bør gjennomføres snarest
Prioritet 2 Viktig tiltak. Bør gjennomføres
Prioritet 3 Ganske viktig tiltak. Kan gjennomføres senere når økonomien tillater det
Prioritet 4 Mindre viktig tiltak
Prioritet 5 Uviktig tiltak

Tiltakene vises etter arbeidsgruppens prioritering.

<table>
<thead>
<tr>
<th>Prioritet</th>
<th>Tiltak</th>
<th>Total nettoeff.</th>
<th>Tiltakskostnad</th>
<th>Ansvar for gjennomføring</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Implementere overvåkning av nettverk og Snow</td>
<td>Moderat</td>
<td>Ubertydlig</td>
<td>Gustav Bellika</td>
</tr>
<tr>
<td>1</td>
<td>Verifisere at antivirus oppdatering omfatter Snow</td>
<td>Moderat</td>
<td>Ubertydlig</td>
<td>Per Atle Bakkevoll</td>
</tr>
<tr>
<td>1</td>
<td>Implementere Snow på alle legekontor</td>
<td>Moderat</td>
<td>Ubertydlig</td>
<td>Gustav Bellika</td>
</tr>
<tr>
<td>1</td>
<td>Implementere endringsprosedyre for labtest rapportering</td>
<td>Moderat</td>
<td>Ubertydlig</td>
<td>Lars Ilebrekke</td>
</tr>
<tr>
<td>1</td>
<td>Dokumentere kontroll av SW</td>
<td>Moderat</td>
<td>Ubertydlig</td>
<td>Per Atle Bakkevoll</td>
</tr>
<tr>
<td>1</td>
<td>Implementere oppdateringsprosedyrer</td>
<td>Moderat</td>
<td>Ubertydlig</td>
<td>Lars Ilebrekke</td>
</tr>
<tr>
<td>1</td>
<td>Implementere driftsprosedyre</td>
<td>Moderat</td>
<td>Ubertydlig</td>
<td>Gustav Bellika</td>
</tr>
<tr>
<td>1</td>
<td>Innføre skrivekontroll på konfig-filer</td>
<td>Moderat</td>
<td>Ubertydlig</td>
<td>Per Atle Bakkevoll</td>
</tr>
<tr>
<td>1</td>
<td>Definere og implementere konfig. krav</td>
<td>Moderat</td>
<td>Ubertydlig</td>
<td>Gustav Bellika</td>
</tr>
<tr>
<td>1</td>
<td>Definere krav for sikring av laptop</td>
<td>Ubertydlig</td>
<td>Ubertydlig</td>
<td>Per Atle Bakkevoll</td>
</tr>
<tr>
<td>1</td>
<td>Fysisk sikre PO serveren</td>
<td>Ubertydlig</td>
<td>Ubertydlig</td>
<td>Per Atle Bakkevoll</td>
</tr>
<tr>
<td>1</td>
<td>Installasjon på alle kontor</td>
<td>Ubertydlig</td>
<td>Ubertydlig</td>
<td>Gustav Bellika</td>
</tr>
</tbody>
</table>
Den tiltakskostnad som gruppen har foreslått er en grov prioritering og tar bare hensyn til det beskrevne tiltaket. Dersom et tiltak fører til nye tiltak for å øke sikkerheten, er disse tiltakskostnadene naturligvis ikke tatt med.

**Kommende aktiviteter:**
De ansvarlige planlegger og gjennomfører sine egne tiltak. Oppfølgning skal skje senest (Dato).

**Konklusjon**
Gitt at alle tiltak blir implementert med unntak av ”slå på kopisperre på EPJ” vil sannsynligheten for at brudd på konfidensialitet, kvalitet, integritet og tilgang være innenfor det akseptable slik at systemet kan settes i produksjon selv om ”kopisperre” ikke er implementert i EPJ. Tiltaket må imidlertid fullføres.

Gustav Bellika
Analyseleder
Hovedrapport

1 Generelt

1.1 Formålet
Formålet er å gjennomføre en profesjonell men likevel rask risikoanalyse på analyseobjektet.

2 Kort om analysemetoden SBA SCENARIO
Metoden som brukes ved analysen er SBA SCENARIO, som inngår i en pakke med metoder, teknikker og hjelpemidler for kvantitative sikkerhetsanalyser på mange ulike områder.

SBA SCENARIO bygger på en scenarioteknikk som idag er den mest framgangsrike metoden for sårbarhetsanalyser.

SBA SCENARIO gir på kort tid og med lav kostnad muligheter til å finne og analysere mangler i sikkerheten samt foreslå beskyttelsestiltak for å redusere sårbarheten.

SBA SCENARIO identifiserer og kvantiserer manglene konsekvenser, tiltakenes kostnader og effektivitet, samt dokumenterer analysen.

SBA SCENARIO inneholder følgende arbeidsstrinn:
- Planlegging av analysen og opplæring av deltagere i scenarioteknikk
- Etablering av arbeidsgrupper
- Agenda for analysen
- Kreativ ”brainstorming” for å finne fram til tenkelige hendelser
- Valg av 5-10 scenariohendelser per gruppe
- Beskrivelse av scenerier
- Avdekking av scenarienes konsekvenser
- Identifisering av mangler som påvirker scenarioforløpet
- Valg og prioritering av tiltak mot manglene
- Innhenting av preliminær standardrapport

Skriveansvarlige og oppdragsgiveren kompletterer og tar fram en sluttrapport.

3 Forberedelser av analysen

3.1 Analyseleder
Gustav Bellika

3.2 Analyse oppgave
Sikkerhet for installasjon og bruk av SNOW primærlegekontor

3.3 Antall grupper i analysen
Angitt antall grupper: 1
3.4 Analyseobjekt
Snow

3.5 Type av analyse
Analysen er gjennomført som Risokovindu.

4 Arbeidsgrupper og deltakere

4.1 Gruppe 1
Navn: Snow gr 1
Deltakere: Anders Baardsgaard
Funksjon: NHN
Deltakere: Lars Ilebrekke
Funksjon: NST
Deltakere: Erlend Bønes
Funksjon: NST
Deltakere: Per Atle Bakkevoll
Funksjon: NST
Deltakere: Per Bruvold
Funksjon: UNN

5 Scenarier

5.1 Antall scenarier per type
Forsinkelse/avbrudd/tap: 4
Uautorisert bruk: 3
Manglende kvalitet: 4
Tilgjengelighet: 3

5.2 Liste over konsekvenser
Ubetydlig: 12
Moderat: 7
Stor: 11
Katastrofal: 0

5.3 Prioritering av scenariene etter risikokostnader

<table>
<thead>
<tr>
<th>Tittel</th>
<th>Frekvens</th>
<th>Skadekostnad</th>
<th>Risikokostnad</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feilaktig data presenteres</td>
<td>Høy</td>
<td>Høy</td>
<td>Moderat</td>
</tr>
<tr>
<td>Dårlig kvalitet på helsehjelp</td>
<td>Moderat</td>
<td>Høy</td>
<td>Moderat</td>
</tr>
<tr>
<td>Pasientdata slettes</td>
<td>Moderat</td>
<td>Høy</td>
<td>Moderat</td>
</tr>
<tr>
<td>PO-server blir kompromittert</td>
<td>Moderat</td>
<td>Høy</td>
<td>Moderat</td>
</tr>
<tr>
<td>Pasientinfo blir tilgjengelig for uvedkommade</td>
<td>Lav</td>
<td>Høy</td>
<td>Moderat</td>
</tr>
</tbody>
</table>
5.4 Grafisk visning av scenariene

<table>
<thead>
<tr>
<th>Svært høy</th>
<th>Høy</th>
<th>Moderat</th>
<th>Libetydig</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>N1</td>
<td>N2-N4</td>
<td>N5</td>
</tr>
</tbody>
</table>

N5: Feilaktig data presenteres
N4: PO-server blir kompromittert
N3: Pasientdata slettes
N2: Dårlig kvalitet på helsehjelp
N1: Pasientinfo blir tilgjengelig for uvedkommende

Figur 1. X akse – frekvens, Y akse - skadekostnad

6 Mangler
Manglene nedenfor er oppdatert forløpende ettersom tiltakene har vært gjennomført. Gjenstående tiltak er skrevet i rød skriftfarge.

6.1 Prioritering av manglene etter mangelkostnader

<table>
<thead>
<tr>
<th>Mangel</th>
<th>OK?</th>
<th>Tiltak</th>
<th>Beskrivelse</th>
<th>Mangelkostnad</th>
<th>Scenario</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manglende krav om anti virus oppdatering</td>
<td>OK</td>
<td>PO server vedlikeholdes en gang pr måned.</td>
<td>Moderat</td>
<td></td>
<td>Feilaktig data presenteres</td>
</tr>
<tr>
<td>Mangler prosedyre for overvåkning av nett</td>
<td>OK</td>
<td>Vi tar ut meldingsstatistikk på PO og legekontor. Oppdateringstjenesten holder oversikt over hvilke servere som ikke er online. Oppdateres daglig. Norsk helsenett overvåker helsenettet.</td>
<td>Moderat</td>
<td>Feilaktig data presenteres</td>
<td></td>
</tr>
<tr>
<td>Mangler datostempling av datagrunnlag</td>
<td>OK</td>
<td>Denne er synlig i klienten</td>
<td>Data som presenteres mangler tid når de er &quot;tatt&quot;</td>
<td>Moderat</td>
<td>Feilaktig data presenteres</td>
</tr>
<tr>
<td>Manglende dekningsgrad</td>
<td>OK</td>
<td>Rekruttering av legekontor pågår</td>
<td>Manglende dekningsgrad fordi ikke alle legekontor rapporterer eller tar i bruk Snow</td>
<td>Moderat</td>
<td>Feilaktig data presenteres</td>
</tr>
<tr>
<td>Mangler prosedyre for endring av labtest rapportering</td>
<td>OK</td>
<td>Prosedyre for oppdatering av analysekoder er implementert</td>
<td>Moderat</td>
<td>Feilaktig data presenteres</td>
<td></td>
</tr>
<tr>
<td>Mangel</td>
<td>OK?</td>
<td>Tiltak</td>
<td>Beskrivelse</td>
<td>Mangelkostnad</td>
<td>Scenario</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>-----</td>
<td>------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------</td>
<td>---------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Mangler verifisering av SW</td>
<td>OK</td>
<td>Oppdateringstjeneste er implementert</td>
<td></td>
<td>Moderat</td>
<td>Feilaktig data presenteres</td>
</tr>
<tr>
<td>Mangler dokumentasjon av systemet</td>
<td></td>
<td>Mangler Dokumentasjon av konsekvenser ved konfigurasjonsendringer (Plugin)</td>
<td></td>
<td>Moderat</td>
<td>PO-server blir compromittert</td>
</tr>
<tr>
<td>Mangler verifisering av konfigurasjon</td>
<td>OK</td>
<td>Konfigurasjonsklasse i openfire er implementert (gjelder alle servere). Klausul om konfigurasjonsendringer i dokumentasjon til legekontor.</td>
<td>Konfig av serveren er for åpen/sårbar</td>
<td>Moderat</td>
<td>PO-server blir compromittert</td>
</tr>
<tr>
<td>Mangler oppdateringsprosedyre</td>
<td>OK</td>
<td>Automatisk Oppdateringsprosedyre er beskrevet (gjøres en gang pr. Måned på PO)</td>
<td>PO serveren mangler prosedyrer for endring av systemet og oppdateringer</td>
<td>Moderat</td>
<td>PO-server blir compromittert</td>
</tr>
<tr>
<td>Mangler fysisk sikring av server</td>
<td>OK</td>
<td>PO server er fysisk sikret i et låst skap.</td>
<td>Serveren står i et ulåst rom på dagtid under pilotdrift</td>
<td>Moderat</td>
<td>PO-server blir compromittert</td>
</tr>
<tr>
<td>Mangler krav om oppdatert anti virus sw</td>
<td>OK</td>
<td>Klausul i ”Driftsrutiner og kontroll” dokument for legekontor</td>
<td></td>
<td>Moderat</td>
<td>Pasientdata slettes</td>
</tr>
<tr>
<td>Mangler skrivekontroll på konfig. filer</td>
<td>OK</td>
<td>Kun administrator og Snow bruker på server har tilgang til å endre konfigurasjon.</td>
<td></td>
<td>Moderat</td>
<td>Pasientdata slettes</td>
</tr>
<tr>
<td>Mangler fysisk sikring av laptop pc</td>
<td>OK</td>
<td>Klausul i dokument: Funk ansatte og systemadm. skal ha tilgang til systemet.</td>
<td></td>
<td>Moderat</td>
<td>Pasientdata slettes</td>
</tr>
<tr>
<td>Mangelfull brukeropplæring</td>
<td>OK</td>
<td>Opplæringsvideoer er laget. legekontor klient gjenstår (ennå ikke utviklet). System administratorer må lese dokument om driftsrutiner og kontroll.</td>
<td></td>
<td>Moderat</td>
<td>Pasientdata slettes</td>
</tr>
<tr>
<td>Mangler prosedyre for oppdatering av Snow</td>
<td>OK</td>
<td>Automatisk oppdateringstjeneste er implementert.</td>
<td></td>
<td>Moderat</td>
<td>Pasientdata slettes</td>
</tr>
<tr>
<td>Mangler driftsprosedyre</td>
<td>OK</td>
<td>Driftsprosedyre er beskrevet for legekontor server.</td>
<td>Driftsprosedyre som omfatter oppdatering av os og antivirus, herunder kontroll av meldingsutveksling</td>
<td>Ubetydlig</td>
<td>Dårlig kvalitet på helsehjelp</td>
</tr>
<tr>
<td>Mangler konfig. krav til uttrekksprogramvare</td>
<td>OK</td>
<td>Utrekksprogram har kun lesetilgang. Låsproblematikk testet uten å kunne fremprovosere feil.</td>
<td>Sette opp slik at lås-problematikk på EPJ unngås</td>
<td>Ubetydlig</td>
<td>Dårlig kvalitet på helsehjelp</td>
</tr>
<tr>
<td>Mangel</td>
<td>OK?</td>
<td>Tiltak</td>
<td>Beskrivelse</td>
<td>Mangelkostnad</td>
<td>Scenario</td>
</tr>
<tr>
<td>----------------------------------------------------</td>
<td>------</td>
<td>---------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------</td>
<td>-----------------------------------------------</td>
</tr>
<tr>
<td>Mangelfull utbredelse og bruk av Snow</td>
<td></td>
<td>Rekruttering av legekontor pågår.</td>
<td>Mangler en rutine som beskriver hvordan varsling og bruk av informasjon skal gjøres om systemet ikke er tilgjengelig</td>
<td>Ubetdylig</td>
<td>Dårlig kvalitet på helsehjelp</td>
</tr>
<tr>
<td>Mangler nødrutine</td>
<td>OK</td>
<td>Nødrutine er beskrevet.</td>
<td></td>
<td>Ubetdylig</td>
<td>Dårlig kvalitet på helsehjelp</td>
</tr>
<tr>
<td>Mangler krav til øvrig infrastruktur</td>
<td>OK</td>
<td>Server versjoner / konfigurasjoner som støttes, port, nettverk, brannmur, antivirus, server oppstart, minnekrav beskrevet i dokument &quot;Driftsrutiner og kontroll&quot;. Terminalserver konfigurasjoner er ikke dekket.</td>
<td></td>
<td>Ubetdylig</td>
<td>Dårlig kvalitet på helsehjelp</td>
</tr>
<tr>
<td>Mangler driftsovervåkning</td>
<td>OK</td>
<td>Implementert. PO server + legekontor overvåkes via oppdateringstjenesten.</td>
<td></td>
<td>Ubetdylig</td>
<td>Dårlig kvalitet på helsehjelp</td>
</tr>
<tr>
<td>Mangler dokumentasjon av systemet</td>
<td>OK</td>
<td>Implementert. PO server + legekontor overvåkes via oppdateringstjenesten.</td>
<td>Konfigurasjonskart og systembeskrivelse må nedtegnes.</td>
<td>Ubetdylig</td>
<td>Pasientinfo blir tilgjengelig for uvedkommende</td>
</tr>
<tr>
<td>Mangler sperre av kopifunksjon i EPJ</td>
<td>OK</td>
<td>Klausul om aktivering av kopisperre beskrevet i &quot;Driftsrutiner og kontroll&quot;</td>
<td>Kopifunksjonen må kunne sperres i EPJ på legekontoret</td>
<td>Ubetdylig</td>
<td>Pasientinfo blir tilgjengelig for uvedkommende</td>
</tr>
<tr>
<td>Mangler prosedyre for oppdatering PC</td>
<td>OK</td>
<td>Klausul om oppdatering av OS og antivirus på klient maskiner er beskrevet i &quot;driftsrutiner og kontroll dokument&quot;</td>
<td>Oppdatering av os og virusbeskyttelse på pc må beskrives og gjennomføres. Prosedyren bør også omfatte kontroll av systemkomponenter</td>
<td>Ubetdylig</td>
<td>Pasientinfo blir tilgjengelig for uvedkommende</td>
</tr>
<tr>
<td>Mangler opplæring</td>
<td>OK</td>
<td>Opplæringsvideo er laget.</td>
<td>Brukere får ikke nødvendig opplæring i bruken av systemet</td>
<td>Ubetdylig</td>
<td>Pasientinfo blir tilgjengelig for uvedkommende</td>
</tr>
<tr>
<td>Mangler prosedyre for oppgradering</td>
<td>OK</td>
<td>Automagisk oppdateringstjeneste implementert. Procedyre for oppdatering er beskrevet.</td>
<td>Procedyre for oppgradering må beskrive hvilke kontroller som skal gjøres etter at en oppdatering er utført</td>
<td>Ubetdylig</td>
<td>Pasientinfo blir tilgjengelig for uvedkommende</td>
</tr>
</tbody>
</table>

Summen av mangelkostnadene for alle manglene som tillhører et scenario tilsvarer risikokostnaden for scenariet.
7 Tiltak

7.1 Grafisk visning av tiltakene

7.2 Prioritering av tiltakene

Tiltakene vises etter arbeidsgruppens prioritering og med verktøyets prioritering i parentes:

<table>
<thead>
<tr>
<th>Prioritet</th>
<th>Total nettoeff.</th>
<th>Scenario</th>
<th>Tiltak</th>
<th>Mangel</th>
<th>Effekt</th>
<th>Kostnad</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 (1)</td>
<td>Moderat</td>
<td>Feilaktig data presenteres</td>
<td>Implementere overvåkning av nettverk og Snow</td>
<td>Mangler prosedyre for overvåkning av nett</td>
<td>Ubetydlig</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Manglende dekningsgrad</td>
<td>Ubetydlig</td>
<td></td>
</tr>
<tr>
<td>1 (3)</td>
<td>Moderat</td>
<td>Feilaktig data presenteres</td>
<td>Verifisere at antivirus oppdatering omfatter Snow</td>
<td>Manglende krav om antivirus oppdatering</td>
<td>Ubetydlig</td>
<td></td>
</tr>
<tr>
<td>1 (4)</td>
<td>Moderat</td>
<td>Feilaktig data presenteres</td>
<td>Implementere Snow på alle legekontor</td>
<td>Manglende dekningsgrad</td>
<td>Ubetydlig</td>
<td></td>
</tr>
<tr>
<td>1 (5)</td>
<td>Moderat</td>
<td>Feilaktig data presenteres</td>
<td>Implementere endringsprosedyre for labtest rapportering</td>
<td>Mangler prosedyre for endring av labtest rapportering</td>
<td>Ubetydlig</td>
<td></td>
</tr>
<tr>
<td>1 (6)</td>
<td>Moderat</td>
<td>Feilaktig data presenteres</td>
<td>Dokumentere kontroll av SW</td>
<td>Mangler verifisering av SW</td>
<td>Ubetydlig</td>
<td></td>
</tr>
<tr>
<td>Prioritet</td>
<td>Total nettoeff.</td>
<td>Scenario</td>
<td>Tiltak</td>
<td>Mangel</td>
<td>Effekt</td>
<td>Kostnad</td>
</tr>
<tr>
<td>-----------</td>
<td>----------------</td>
<td>----------</td>
<td>--------</td>
<td>--------</td>
<td>--------</td>
<td>---------</td>
</tr>
<tr>
<td>1 (7)</td>
<td>Moderat</td>
<td>PO-server blir kompromittert</td>
<td>Implementere oppdateringsprosedyrer</td>
<td>Mangler verifisering av konfigurasjon</td>
<td>Ubetydlig</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>PO-server blir kompromittert</td>
<td>Mangler oppdateringsprosedyre</td>
<td>Ubetydlig</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 (8)</td>
<td>Moderat</td>
<td>Dårlig kvalitet på helsesjelp</td>
<td>Implementere driftsprosedyre</td>
<td>Mangler nødrutine</td>
<td>Ubetydlig</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Dårlig kvalitet på helsesjelp</td>
<td>Mangler driftsøvervåkning</td>
<td>Ubetydlig</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Dårlig kvalitet på helsesjelp</td>
<td>Mangler driftsprosedyre</td>
<td>Ubetydlig</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 (9)</td>
<td>Moderat</td>
<td>Pasientdata slettes</td>
<td>Innføre skrivekontroll på konfig-filer</td>
<td>Mangler prosedyre for oppdatering av Snow</td>
<td>Ubetydlig</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Pasientdata slettes</td>
<td>Mangler skrivekontroll på konfig-filer</td>
<td>Ubetydlig</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 (10)</td>
<td>Moderat</td>
<td>Dårlig kvalitet på helsesjelp</td>
<td>Definere og implementere konfig. krav</td>
<td>Mangler krav til øvrig infrastruktur</td>
<td>Ubetydlig</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Dårlig kvalitet på helsesjelp</td>
<td>Mangler konfig. krav til uttrekksprogramvare</td>
<td>Ubetydlig</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 (11)</td>
<td>Ubetydlig</td>
<td>Pasientdata slettes</td>
<td>Definere krav for sikring av laptop</td>
<td>Mangler fysisk sikring av laptop pc</td>
<td>Ubetydlig</td>
<td></td>
</tr>
<tr>
<td>1 (12)</td>
<td>Ubetydlig</td>
<td>PO-server blir kompromittert</td>
<td>Fysisk sikre PO serveren</td>
<td>Mangler fysisk sikring av server</td>
<td>Ubetydlig</td>
<td></td>
</tr>
<tr>
<td>1 (13)</td>
<td>Ubetydlig</td>
<td>Dårlig kvalitet på helsesjelp</td>
<td>Installasjon på alle kontor</td>
<td>Mangelfull utbredelse og bruk av Snow</td>
<td>Ubetydlig</td>
<td></td>
</tr>
<tr>
<td>1 (14)</td>
<td>Ubetydlig negativ</td>
<td>Pasientinfo blir tilgjengelig for uvedkommende</td>
<td>Implementere opplæringsopplegg</td>
<td>Mangler dokumentasjon av systemet</td>
<td>Ubetydlig</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Pasientinfo blir tilgjengelig for uvedkommende</td>
<td>Mangler opplæring</td>
<td>Ubetydlig</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1 (15)</td>
<td>Moderat negativ</td>
<td>Pasientinfo blir tilgjengelig for</td>
<td>Slå på kopisperre på</td>
<td>Mangler sperre</td>
<td>Høy</td>
<td></td>
</tr>
<tr>
<td>uvedkommende</td>
<td>EPJ</td>
<td>kopifunksjon i EPJ</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------------</td>
<td>-----</td>
<td>-------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2 (2) Moderat</td>
<td>Feilaktig data presenteres</td>
<td>Visualisere datostempling på klient</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Mangler datostempling av datagrunnlag</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Ubetydlig</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

7.3 Type beskyttelse
Forebyggende: 15
Etterforske: 0
Begrensende: 0
Bestilling: 0

Gustav Bellika
Analyseleder
Risikovurdering

Fjernadministrasjon av Snow PO-tjener
- Et tillegg til risikoanalysen

Versjon 1.0

Dato
09.07.13

Eva Henriksen
Benn Molund
Torje Henriksen
### Forkortelse og forklaring

<table>
<thead>
<tr>
<th>Forkortelse</th>
<th>Forklaring</th>
</tr>
</thead>
<tbody>
<tr>
<td>NST</td>
<td>Nasjonalt senter for samhandling og telemedisin [1]</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtuelt Privat Nettverk – Teknologi for å koble seg til et beskyttet nett gjennom en kryptert forbindelse.</td>
</tr>
<tr>
<td>SSH</td>
<td>Secure shell – en måte å gjøre kryptert pålogging mot en server ved hjelp av et nøkkelpar eller brukernavn og passord</td>
</tr>
<tr>
<td>NHN</td>
<td>Norsk Helsenett SF [2]</td>
</tr>
<tr>
<td>HTTP</td>
<td>Hypertext Transfer Protocol – Protokollen som brukes når man “surfer” på Internett</td>
</tr>
<tr>
<td>SMTP</td>
<td>Simple Mail Transfer Protocol – Protokoll for å sende e-post</td>
</tr>
<tr>
<td>UNN</td>
<td>Universitetssykehuset Nord-Norge [3]</td>
</tr>
<tr>
<td>Signerings-laptop</td>
<td>En dedikert PC brukt utelukkende for å signere programvareoppdateringer som distribueres fra PO-server.</td>
</tr>
<tr>
<td>AMS</td>
<td>Avdeling for mikrobiologi og smittevern, UNN</td>
</tr>
</tbody>
</table>

Tabell 1: Forkortelser og forklaringer

### Introduksjon

Tjenesten vi analyserer i dette dokumentet er fjernadministrasjon av Snow-prosjektets PO-server i Helsenettet. Situasjonen i dag er at driftspersonell må være fysisk ved serveren for å kunne administrere den. Fordi personalet som drifter Snow PO-server ikke lenger vil være lokalisert hvor serveren er, vil det i framtiden bli svært vanskelig å drive vedlikehold uten fjerntilgang.

På et senere tidspunkt skal PO-serveren flyttes til et segment av Helsenettet hvor man forventer at det er tilrettelagt for fjernadministrasjon av servere, men per i dag er det i følge NHN ikke mulig å tilby fjerntilgang til serveren gjennom deres nett eller tjenester.

En midlertidig løsning hvor man kobler PO-serveren til et fjernstyringsnett separat fra Helsenettet er derfor foreslått. Resten av dokumentet er en beskrivelse og risikovurdering av denne løsningen.

### Beskrivelse av tjenesten

Snow er et distribuert system som agregerer data fra avdeling for mikrobiologi og smittevern (AMS) ved UNN, og også noen legekontor. Denne statistikken sendes så til PO-server som distribuerer disse på Helsenett og til Internett. Det er ingen sensitive data på PO-serveren. Alle data som kommer til PO-serveren er aggregerte, og det er de samme dataene som distribueres til Internett via SMTP. Snow-systemet er beskrevet i større detalj i den opprinnelige risikoanalysen [4].
**Fjernstyring**

Fjernstyringen planlegges implementert ved å koble PO-serveren til et fjernstyringsnett separat fra Helsenettet. En arbeidsstasjon kan nå fjernstyringsnettet ved hjelp av VPN, og får så tilgang til å nå PO-serveren over SSH. Se Figur 1.

![Diagram](image)

**Figur 1**: Oversikt over servere i Snow-systemet samt trafikken mellom dem. Fjernadministrasjonsløsningen er tegnet inn i blått
Fjernstyringsnettet kan defineres som hele Internett, et lokalt nett slikt som et vanlig bedriftsnett, eller et dedikert nett kun for dette formålet. Kun de som er tilkoblet fjernstyringsnettet har mulighet til å prøve å logge seg på PO-serveren.

Vi ønsker å bruke NST sitt driftsnett som fjernstyringsnett. Det vil si at alle ansatte ved NST har tilgang til det vi definerer som fjernstyringsnettet. Fjernstyringsnettet kan nåes over VPN fra Internett over hele verden.

Selv om alle NST-ansatte kan nå fjernstyringsnettet, vil det kun være de med driftsansvar for PO-serveren som kan logge seg inn på selve serveren, da det kun er de som har brukernavn, passord og nøklene som skal til for å logge seg på. Innloggingen skjer over SSH. Det er helt avgjørende for sikkerheten av løsningen at brukernavn, passord og nøkler holdes hemmelige, og at tilgang kun gis til de som skal ha det.

Grunnen til at vi ønsker å bruke NST sitt nett som fjernstyringsnett i stedet for et dedikert nett, er kostnadene involvert ved å lage og vedlikeholde et separat fjernstyringsnett. Dette er særlig med tanke på at dette er en midlertidig løsning.

Neste seksjon oppsummerer og konkretiserer hvilken informasjon man trenger for å kunne nå og logge seg på PO-server.

**Krav for å klare å logge seg på PO-server ved hjelp av fjerntilgang:**

For å fjernadministrere PO-serveren, må administrator:

1. Være koblet til Internett
2. Installere VPN-programvare og ha sertifikatene utstedt av NST
3. Ha et brukernavn og passord hos NST
4. Brukernavn, personlig passord, nøkkelfil og personlig passord til nøkkelfil på PO-server

Alle ansatte ved NST oppfyller punkt 1-3, mens kun de med driftsansvar for PO-server oppfyller punkt 4.

For å legge ut ny programvare for oppdatering av Snow-systemet, må man i tillegg ha tilgang til signerings-laptop og brukernavn og passord til denne og passordet til privat krypteringsnøkkel.

**Sikkerheten i løsningen forutsetter at brukernavn, passord og nøkler holdes hemmelig.**

**Detaljer vedrørende PO-servers tilkobling til fjernadministrasjonnett**

PO-server er fra før av koblet til sitt segment av Helsenettet med et nettverkskort med IP-adresse 91.186.92.2.

For å koble PO-server til fjernadministrasjonsnettet, vil man sette inn et nytt fysisk nettverkskort hvor man kobler dette kortet til fjernadministrasjonnettet. Dette nettverkskortet vil få en IP-adresse i det lokale NST-nettet 172.21.15.0/24.

PO-server har altså to fysiske nettverkskort med separate adresser i separate nettverk. Ruting mellom disse nettene er ikke tillatt.

I figur 1 på side 4 kan man også se at det står en brannmur mellom fjernadministrasjonsnettet og PO-server. Denne brannmuren tillater kun trafikk på SSH-porten (TCP/22). Videre vil SSH kun være
aktivert kun for fjernstyringsnettet, og ikke for nettverkskortet som står i Helsenette.

**Analyse**

Risikoanalyser legger til grunn at beskrivelsen ovenfor er korrekt. Denne analysen vil ikke beskrive eller foreslå tiltak som allerede er implementert eller beskrevet over. Spesielt kan det nevnes at analysen forutsetter at brukernavn, passord, nøkler samt passord til nøkler holdes hemmelig. Og at laptop brukt for signering av programvare holdes *offline* og innelåst.


Id-ene som brukes for å identifisere hendelser er definert annerledes i dette tillegget. Her betyr Id-ene som begynner på A at det er et nytt moment, mens Id-ene som begynner med B er gamle momenter hvor vi ønsker å vurdere om risiko har endret seg på grunn av endringene som gjøres.

På de neste sidene følger trusseltabell (Tabell 2) og risikomatrise (Tabell 3), etterfulgt av en kort diskusjon og konklusjon.
<table>
<thead>
<tr>
<th>Id</th>
<th>Trussel, hendelse</th>
<th>Årsak</th>
<th>Sannsynlighet</th>
<th>Konsekvens</th>
<th>Risiko</th>
<th>Kommentar</th>
</tr>
</thead>
</table>
| A1 | Fjernstyringsnett rutes inn i Helsenettet.  
Det vil si at alle i NSTnettet har mulighet til å nå nettverkssegmentet PO-server står i. | Noen med root-tilgang gjør dette med vilje.  
Systemadministrator gjør feil  
Feil i operativsystem | Lav  
Det er vanskelig å se for seg hvorfor noen ville gjøre dette med vilje.  
Det er ingen gevinst på å gjøre dette.  
Det er heller ikke noe som er enkelt å gjøre ved uhell. | Liten  
Liten konsekvens fordi det er ingen andre servere i dette segmentet, og trafikk vil uansett stoppes av brannmurene som nettet befinner seg bak. | Lav |  |
| B1 | Noen kjerer med vilje mange oppdrag og belaster servere på legekontor og lab  
Uvedkommende får tilgang til PO-server og ønsker å sabotere for prosjektet. | Uvedkommende får tilgang til PO-server og ønsker å sabotere for prosjektet.  
Det er ingen gevinst utover sabotasje av servere i form av denial-of-service. | Lav  
Det er ingen gevinst utover sabotasje av servere i form av denial-of-service.  
Kan gå ut over legekontorenes evne til å utføre sitt daglige arbeid pga treghet i systemet | Alvorlig  
Går ut over ryktet til NST og Snow  
Kan gå ut over legekontorenes evne til å utføre sitt daglige arbeid pga treghet i systemet | Middels | Konsekvensen anses som alvorlig fordi den kan påvirke ikke bare NST og Snow, men også andre partnere slik som legekontor og mikrobiologilab.  
Akseptabel da vi er usikre på i hvor stor grad det er mulig å overbelaste produksjonssystemene ved å kjøre oppdrag fra Snowsystemet.  
I tillegg til at sannsynligheten regnes som lav. |
<table>
<thead>
<tr>
<th>B2</th>
<th>Noen saboterer PO-server</th>
<th>Noen får tilgang til PO-server og sletter enten systemfiler eller Snow-spesifike filer</th>
<th>Lav</th>
<th>Ingen gevinst for angriper.</th>
<th>Moderat</th>
<th>Tjenesten går ned. Ødelegger merkenavnet Snow og NSTs rykte</th>
<th>Lav</th>
</tr>
</thead>
<tbody>
<tr>
<td>B3</td>
<td>Noen endrer rapportene som publiseres</td>
<td>Noen får tilgang til PO-server og endrer dem</td>
<td>Lav</td>
<td>Ingen gevinst for angriper.</td>
<td>Moderat</td>
<td>Tjenesten distribuerer feil data. Ødelegger for ryktet til Snow og NST</td>
<td>Lav</td>
</tr>
</tbody>
</table>

*Tabell 2: Trusseltabell*
<table>
<thead>
<tr>
<th>Sannsynlighet/Konsevens</th>
<th>Liten</th>
<th>Moderat</th>
<th>Alvorlig</th>
<th>Katastrofal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lav</td>
<td>A1, B4</td>
<td>B2, B3</td>
<td>B1</td>
<td></td>
</tr>
<tr>
<td>Middels</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Høy</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Svært høy</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Tabell 3: Risikomatrise. De hvite feltene regnes som akseptable, de lysegrå krever at man følger opp kontinuerlig vurderer tiltak, mens de mørkegrå er uakseptable risikoer som krever tiltak før systemet kan settes i drift.
**Diskusjon**

Ut i fra risikomatrisen i tabell 3 kan man se at alle truslene har lav risiko. Dette kommer først og fremst av at sannsynligheten regnes som lav for alle tilfellene. Den lave sannsynligheten forutsetter at alle relevante brukernavn, passord og nøkler holdes hemmelige. I tillegg har vi ikke kunnet identifisere sterke motiver for å utnytte truslene.

**Konklusjon**

Vi kan ikke se at fjernadministrasjonsløsningen slik den er beskrevet i dette dokumentet vil føre til en betydelig høyere risiko for noen av partene i Snow-systemet.

**Referanser**

1: Nasjonalt senter for samhandling og telemedisin, http://www.telemed.no
2: Norsk Helsenett SF, http://www.nhn.no
Risk Assessment Report

Configuration service for SNOW appliances using Chef and reverse SSH tunnel

1.0
20.04.2016

Andrius Budrionis
Torje Henriksen
Joseph Stephen Hurley
Johan Gustav Bellika

This document is based on the Risk Assessment template developed at the Norwegian Centre for Integrated Care and Telemedicine
Summary

Background for risk analysis
The separation of the SNOW system components from the critical systems in the GP offices called for a more sustainable and scalable way for configuring the distributed nodes. Currently SNOW GP office nodes are distributed as standalone appliance boxes, which need to be plugged into the data network to function. Chef\(^1\) was selected as a framework for automating the setup and configuration of the SNOW appliance boxes.

This risk assessment analyses the threats introduced by the use of Chef and reverse SSH tunnel for managing the distributed SNOW infrastructure. Other aspects of the system have already been discussed in previously performed risk assessments and therefore are out of the scope of this document.

Conclusions
Eleven threats introduced by the use of Chef and reverse SSH tunnel for managing the SNOW infrastructure were identified. All of them were characterized as acceptable, given the currently implemented security mechanisms.

\(^1\) https://www.chef.io
Contents
Summary................................................................................................................................. 2
Background for risk analysis ................................................................................................. 2
Conclusions ............................................................................................................................. 2
1. Description of the system/service .................................................................................... 4
   1.1. Data handled by the Chef server ............................................................................... 5
   1.2. Implemented security mechanisms ........................................................................ 5
2. Definition of likelihood, consequences and risk levels ................................................... 5
   2.1. Likelihood .................................................................................................................. 5
   2.2. Consequences ........................................................................................................... 7
   2.3. Risk levels ................................................................................................................. 8
3. Identification and evaluation of threats ............................................................................. 9
   3.1. Unauthorized physical access to Chef server ......................................................... 9
   3.2. Unauthorized remote access to Chef server ........................................................... 9
   3.3. Unauthorized upload of cookbooks ......................................................................... 9
   3.4. Unauthorized physical access to SNOW appliance box ....................................... 9
   3.5. Unauthorized remote access to SNOW appliance box through reverse SSH tunnel 9
   3.6. Unauthorized access to configuration data in transfer (read) ............................... 9
   3.7. Unauthorized access to configuration data in transfer (write) ............................. 9
   3.8. Spread of malicious software ............................................................................... 10
   3.9. Chef server is unavailable ...................................................................................... 10
   3.10. Reverse SSH tunnel fails to establish .................................................................. 10
   3.11. Appliance box fails to connect to the Chef server ............................................. 10
4. Conclusions and recommendations .................................................................................. 10
5. References ....................................................................................................................... 11
Appendix A. Threats table ..................................................................................................... 12
Appendix B. Prevention plan ................................................................................................. 14
1. Description of the system/service
SNOW infrastructure consists of computational nodes spread over various networks with different access restrictions (Figure 1). SNOW appliance boxes are deployed in GP offices and process data from electronic health records (EHR) locally. No sensitive patient information leaves the GP office network at any time. Appliance box containing initial software setup is delivered to the GP offices by mail. After the box is connected to the network it contacts the Chef server for configuration data. Every box runs a Chef client, which maintains the connection to the Chef server and executes the instructions defined in cookbooks. Chef server hosts configuration data and setup instruction of all the GP office nodes in the system. Chef clients automatically check Chef server for configuration updates every 30 min. If differences between the current configuration of the node and the one stored on the Chef server is detected, instructions are downloaded and executed. It is important to note that the update of the GP office node is initiated by the node itself (GP office -> Chef server), not the Chef server (Figure 1). SNOW appliance box in the GP office can be instructed to establish a reverse SSH tunnel to a dedicated relay server. Such instructions need to be defined in a cookbook and fetched by a GP office node as a part of a scheduled update. Reverse SSH tunnel enables the system administrator to establish an SSH connection to the appliance box. A new tunnel is created every time a connection to the node is required and destroyed after use (Figure 1).

Figure 1. Architecture of the system
This risk assessment is limited to the configuration mechanisms implemented in the SNOW infrastructure and does not cover other aspects of the system. Many of them have already been covered in previously performed risk assessments [1].

1.1. Data handled by the Chef server
Chef server hosts configuration and update instructions of the GP office nodes. It includes internal IP addresses of the appliance box, EHR database server, relay server for reverse SSH tunnel, etc. Such information is stored in machine-readable objects (cookbooks) containing setup instructions to be executed on the appliance boxes. Addresses of third-party library update servers (Medrave, Chef, Java, etc.) running on the GP office appliance box is defined in cookbooks as well. Call for these updates is initiated by executing the instructions from the cookbook on a GP office node (GP office -> update server). No sensitive patient information reaches Chef server at any time.

1.2. Implemented security mechanisms
Chef server could be used as an entry point to compromise the security of the SNOW infrastructure. The server itself has no access to the GP office nodes and sensitive data, however, uploading a malicious cookbook could result in a security breach. To prevent such incidents, the following security mechanisms/practices are implemented:
1. SSH-based authentication is enforced.
2. Configuration data, stored on the server (ChefVault), is encrypted using public keys of the Chef clients.
3. GP office nodes run on the dedicated hardware physically separated from the critical EHR systems.
4. The connection between the GP office appliance box and the Chef server can only be initiated from the GP office.

Additional security mechanisms are considered according to the needs.

2. Definition of likelihood, consequences and risk levels
This section defines the criteria for evaluating potential threats to the system.

2.1. Likelihood
Four level scale for likelihood (Table 1) and criticality of the consequences (Table 2) were defined and used in the assessment.

Likelihood levels can be described as frequency values or with respect to how easy it is for a person to exploit a threat. For some threats it is easier to think of the likelihood in the form of frequency or a probability value. This may often be the case for threats related to availability, e.g. caused by problems in SW or HW. For other threats it is easier to think of likelihood when related to ease of misuse or mistake, or related to motivation for performing a malicious action. For each threat or unwanted incident we choose the most appropriate column or the column that is easiest to use in order to estimate the likelihood for the threat.
<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Frequency</th>
<th>Ease of misuse Motivation</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Incident may happen several times a day/week</td>
<td>Can be done with minor knowledge about the system; or without any additional equipment being used; or it can be performed by wrong or careless usage</td>
</tr>
<tr>
<td>Moderate</td>
<td>Incident may happen several times a year</td>
<td>Normal knowledge about the system is sufficient; or normally available equipment can be used; or it can be performed deliberately</td>
</tr>
<tr>
<td>Low</td>
<td>No more than one incident per year</td>
<td>Detailed knowledge about the system is needed; or special equipment is needed; or it can only be performed deliberately and by help of internal personnel</td>
</tr>
<tr>
<td>Very low</td>
<td>Less than one incident every two years</td>
<td>Detailed knowledge about the system is needed; or special equipment is needed; or it can only be performed deliberately and by help of internal personnel</td>
</tr>
</tbody>
</table>
2.2. Consequences

Four levels of severity of consequences were defined – Small, Moderate, Serious and Catastrophic. Levels are summarized in Table 2.

<table>
<thead>
<tr>
<th>Consequence</th>
<th>Legal</th>
<th>Economy</th>
<th>Availability</th>
<th>Use of resources</th>
<th>Reputation and trust</th>
<th>Quality of healthcare service</th>
<th>Patient privacy</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Catastrophic</strong></td>
<td>Serious offenses, imprisonment / corporate penalty, Loss of the right to pursue activities</td>
<td>Irreparable financial losses</td>
<td>Two or more days downtime for critical EHR systems</td>
<td>Closing of services, Extensive extra work</td>
<td>Devastating effects on trust and respect</td>
<td>Unsustainable healthcare for patients, with the possibility of loss of life</td>
<td>Privacy violation for large number of patients, influencing life, health and finances</td>
</tr>
<tr>
<td><strong>Serious</strong></td>
<td>Offences, Payment of fines / corporate penalty</td>
<td>Significant economic losses</td>
<td>More than 6 hours unplanned downtime for EHR systems</td>
<td>Extensive work with temporary storage of health records and transfer to production system later, prolonged duration of treatment</td>
<td>Serious loss of reputation, Long-term effects on trust and respect</td>
<td>Insufficient quality of healthcare to many patients, potentially resulting in significant health status decline</td>
<td>Large amounts of sensitive information available to unauthorized persons</td>
</tr>
<tr>
<td><strong>Moderate</strong></td>
<td>Less serious offenses, for example, revealed sensitive information of a small number of patients</td>
<td>Moderate economic losses</td>
<td>Two to 6 hours unplanned downtime of EHR systems or more than 2 days downtime of significant part of SNOW infrastructure node</td>
<td>Extra work with temporary storage of health records and transfer to production system later</td>
<td>Loss of reputation, affecting trust and respect</td>
<td>Obstruction of healthcare practices, Potential non-serious health status decline</td>
<td>Violation of privacy for some patients due to compromised sensitive information</td>
</tr>
<tr>
<td><strong>Small</strong></td>
<td>Minor offenses / Warning</td>
<td>Insignificant economic losses</td>
<td>Less than 2 hours unplanned downtime of EHR systems or more than 1 day downtime for SNOW infrastructure node</td>
<td>Hassles and annoyances</td>
<td>Loss of reputation, Short-term effect on trust and respect</td>
<td>Short-term obstruction of healthcare practices for a small number of patients, No impact on patient health status</td>
<td>Compromise of patient information of low sensitivity</td>
</tr>
</tbody>
</table>
2.3. Risk levels

Three distinct risk levels were defined and used in the risk assessment (Table 3). The risk value for each threat is calculated as the product of consequence and likelihood values, illustrated in a two-dimensional matrix (Table 4).

Based on the acceptance criteria, the risk level High is decided to be unacceptable. Any threat obtaining this risk level must be treated in order to have its risk reduced to an acceptable level. Threats with Low risk level are acceptable, and Medium risks have to be further looked into individually.

Table 3: Definition of risk levels

<table>
<thead>
<tr>
<th>Risk level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>Acceptable risk. The service can be used with the identified threats, but the threats must be observed to discover changes that could increase the risk level</td>
</tr>
<tr>
<td>Medium</td>
<td>Each threat has to be investigated separately. For some threats the risk can be acceptable, but the development of the risk must be monitored on a regular basis, with a following consideration whether necessary measures have to be implemented</td>
</tr>
<tr>
<td>High</td>
<td>Not acceptable risk. The service cannot be in use before risk reducing treatment has been implemented</td>
</tr>
</tbody>
</table>

Table 4: Risk matrix showing the defined risk levels

<table>
<thead>
<tr>
<th>Probability</th>
<th>Consequence: Small</th>
<th>Moderate</th>
<th>Serious</th>
<th>Catastrophic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
</tr>
<tr>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
</tr>
<tr>
<td>Moderate</td>
<td>Low</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>High</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
<td>High</td>
</tr>
</tbody>
</table>
3. Identification and evaluation of threats
This chapter defines the identified threats, their causes and potential mitigation and prevention strategies. Threats are summarized in Appendix A.

3.1. Unauthorized physical access to Chef server
Chef server is hosted by the Norwegian Centre for E-health research following the established maintenance and security practices. Physical access is restricted to authorized personnel, intrusions are unlikely.

3.2. Unauthorized remote access to Chef server
Lost user credentials and SSH keys could provide unauthorized third parties access to the Chef server, where configuration data for all SNOW appliance boxes are stored. Even though it does not give direct access to GP office nodes, the server could be used for gaining insight into deployment of the infrastructure and altering the configuration data to access the deployed appliance boxes. Extensive knowledge of Chef and system configuration is required for a successful attack.

3.3. Unauthorized upload of cookbooks
Uploading a new cookbook to Chef server does not require “root” access. Lost user credentials and SSH keys could allow unauthorized third party to upload malicious cookbooks, which could potentially change the configuration of the appliance boxes. Extensive knowledge of Chef and system configuration is required for a successful attack.

3.4. Unauthorized physical access to SNOW appliance box
A deployed appliance box is located in the server room in the GP office together with the EHR servers, following the same restrictions for physical access. However, due to its size and easy installation, appliance box containing the extracted data might be easier to steal. Moreover, direct access to the box may be used to get control over it, alter the configuration or enable “backdoor” access. It is important to mention, that EHR servers in GP offices are exposed to similar threats.

3.5. Unauthorized remote access to SNOW appliance box through reverse SSH tunnel
SSH tunnel is established from a deployed SNOW appliance box to a dedicated relay server used only for this purpose. The tunnel enables SSH access to the appliance box bypassing the restrictions of NHN HTTP proxy. SSH tunnel can be initiated from:
   a) Chef server, specifying it in the configuration data (threat 5a., Appendix A). Access to Chef server is required to exploit this threat (discussed in 3.1., 3.2. and 3.3.)
   b) Appliance box, after gaining physical access to it and applying malicious configuration (discussed in 3.4.)

3.6. Unauthorized access to configuration data in transfer (read)
Man-in-the-middle attack to gain insight into the configuration data in transfer may provide insight into deployment of the infrastructure (discussed in 3.1. and 3.2.).

3.7. Unauthorized access to configuration data in transfer (write)
Man-in-the-middle attack to gain control over configuration data in transfer may provide a way to alter the configuration of the box (discussed in 3.1., 3.2. and 3.3.).
3.8. Spread of malicious software
Malicious software is referred to as computer viruses, trojans, worms, etc. spreading through different computer systems, damaging data, misusing resources or interfering with functioning of the system. By using Chef server SNOW appliance boxes install and update a list of libraries, frameworks and database systems from locations predefined in cookbooks. All updates are verified by the vendors, minimizing the likelihood of containing malicious software.

3.9. Chef server is unavailable
Chef server may become unavailable due to planned or unplanned reasons. It is important to note that the availability of Chef server does not interfere with the functioning of the SNOW infrastructure. The deployed boxes continue to work using their current configuration until Chef server becomes available.

3.10. Reverse SSH tunnel fails to establish
Changes in network configuration may prevent the establishment of the reverse SSH tunnel. Even though it has no influence on the functioning of the SNOW infrastructure, it disables direct SSH access to the node. The problem may potentially be solved by updating the cookbooks on the Chef server, given that the node can establish the connection to it.

3.11. Appliance box fails to connect to the Chef server
Changes in network configuration may prevent the appliance box from connecting to the Chef server. No updates would be available for the node until network obstructions are identified and fixed or the node is replaced by a new one containing the required configuration.

4. Conclusions and recommendations
Threats to the system introduced by the use of Chef and reverse SSH tunnel were identified and evaluated in SNOW project team meetings 13.04.2016 and 20.04.2016. The following participants were present: Andrius Budrionis, Torje Henriksen, Joseph Stephen Hurley, Johan Gustav Bellika.
Eleven threats were identified and evaluated (Appendix A). Six threats could potentially lead to serious consequences, however the likelihood of them is very low. The rest had small potential consequences. Therefore, all identified threats were assigned an acceptable (low) risk level with the implemented security measures being sufficient to mitigate the consequences (Table 5).
Suggestions for increasing the security of the system are presented in Appendix B, according to the identified threats.
Table 5. Threats and risk levels

<table>
<thead>
<tr>
<th>Consequence: Probability:</th>
<th>Small</th>
<th>Moderate</th>
<th>Serious</th>
<th>Catastrophic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very low</td>
<td>6, 9a, 9e</td>
<td></td>
<td>1, 2, 3, 5a, 7, 8,</td>
<td></td>
</tr>
<tr>
<td>Low</td>
<td>4, 5b, 9b, 9d</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Moderate</td>
<td>9c, 10, 11</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>High</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

5. References
### Appendix A. Threats table

<table>
<thead>
<tr>
<th>ID</th>
<th>Threat / Unwanted incident</th>
<th>Cause</th>
<th>Likelihood</th>
<th>Consequence</th>
<th>Risk level</th>
<th>Acceptable risk</th>
<th>Comments and descriptions of implemented security measures</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Unauthorized physical access to Chef Server</td>
<td>Physical intrusion into the server room for various reasons</td>
<td>Very low</td>
<td>Serious</td>
<td>Low</td>
<td>Yes</td>
<td>Equipment is located in a dedicated server room with restricted access</td>
</tr>
<tr>
<td>2.</td>
<td>Unauthorized remote access to Chef Server (“root rights”) (server encryption keys, public keys of all clients, IP addresses and configurations of all clients)</td>
<td>Lost user credentials and SSH keys</td>
<td>Very low</td>
<td>Serious</td>
<td>Low</td>
<td>Yes</td>
<td>Key-based authentication</td>
</tr>
<tr>
<td>3.</td>
<td>Unauthorized upload of cookbooks</td>
<td>Lost user credentials and SSH keys</td>
<td>Very low</td>
<td>Serious</td>
<td>Low</td>
<td>Yes</td>
<td>Key-based authentication</td>
</tr>
<tr>
<td>4.</td>
<td>Unauthorized physical access to SNOW-box</td>
<td>Physical intrusion into the GP office server room for various reasons</td>
<td>Low</td>
<td>Small with regards to Chef client</td>
<td>Low</td>
<td>Yes</td>
<td>A deployed SNOW appliance box is located in the server room in the GP office, ensuring the same physical access restriction that are applied to EHR servers</td>
</tr>
<tr>
<td>5a.</td>
<td>Unauthorized remote access to SNOW-box through reverse SSH tunnel</td>
<td>SSH tunnel may be initiated by hijacking the Chef server and uploading malicious cookbook, which instructs the remote node to establish a tunnel to a selected host</td>
<td>Very low</td>
<td>Serious</td>
<td>Low</td>
<td>Yes</td>
<td>SSH tunnel is established on-demand and destroyed after use</td>
</tr>
<tr>
<td>5b.</td>
<td></td>
<td>Initiated from the box after gaining physical access (discussed in threat 4)</td>
<td>Low</td>
<td>Small with regards to Chef client</td>
<td>Low</td>
<td>Yes</td>
<td>A deployed SNOW appliance box is located in the server room in the GP office, ensuring the same physical access restriction that are applied to EHR servers</td>
</tr>
<tr>
<td>ID</td>
<td>Threat / Unwanted incident</td>
<td>Cause</td>
<td>Likelihood</td>
<td>Consequence</td>
<td>Risk level</td>
<td>Acceptable risk</td>
<td>Comments and descriptions of implemented security measures</td>
</tr>
<tr>
<td>----</td>
<td>-----------------------------</td>
<td>-------</td>
<td>------------</td>
<td>-------------</td>
<td>------------</td>
<td>-----------------</td>
<td>--------------------------------------------------------</td>
</tr>
<tr>
<td>6</td>
<td>Unauthorized access to configuration data in transfer (read)</td>
<td>Man-in-the-middle attack</td>
<td>Very low</td>
<td>Small</td>
<td>Low</td>
<td>Yes</td>
<td>Configuration data is encrypted on the server using Chef Vault²</td>
</tr>
<tr>
<td>7</td>
<td>Unauthorized access to configuration data in transfer (write)</td>
<td>Man-in-the-middle attack</td>
<td>Very low</td>
<td>Serious</td>
<td>Low</td>
<td>Yes</td>
<td>Configuration data is encrypted on the server using Chef Vault</td>
</tr>
<tr>
<td>8</td>
<td>Spread of malicious software (virus, etc…)</td>
<td></td>
<td>Very low</td>
<td>Serious</td>
<td>Low</td>
<td>Yes</td>
<td>No human factor in the infrastructure</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Infrastructure mostly consists of Linux nodes, Windows nodes run Windows Defender</td>
</tr>
<tr>
<td>9a</td>
<td>Chef server is unavailable</td>
<td>Hardware fail</td>
<td>Very low</td>
<td>Small</td>
<td>Low</td>
<td>Yes</td>
<td>Redundancy, scheduled maintenance</td>
</tr>
<tr>
<td>9b</td>
<td></td>
<td>Electricity fail</td>
<td>Low</td>
<td>Small</td>
<td>Low</td>
<td>Yes</td>
<td>Automatic start up after incident</td>
</tr>
<tr>
<td>9c</td>
<td></td>
<td>Network fail</td>
<td>Moderate</td>
<td>Small</td>
<td>Low</td>
<td>Yes</td>
<td>Automatic recovery of services after the network is back</td>
</tr>
<tr>
<td>9d</td>
<td></td>
<td>Software fail</td>
<td>Low</td>
<td>Small</td>
<td>Low</td>
<td>Yes</td>
<td>Scheduled on-time updates</td>
</tr>
<tr>
<td>9e</td>
<td></td>
<td>DDoS attack</td>
<td>Very low</td>
<td>Small</td>
<td>Low</td>
<td>Yes</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Maintenance</td>
<td>Moderate</td>
<td>Small</td>
<td>Low</td>
<td>Yes</td>
<td>Maintenance is scheduled and short-term</td>
</tr>
<tr>
<td>10</td>
<td>SSH tunnel fails to establish</td>
<td>Networking problems, configuration errors, etc.</td>
<td>Moderate</td>
<td>Small</td>
<td>Low</td>
<td>Yes</td>
<td>Can potentially be fixed through updating the cookbooks on the Chef server</td>
</tr>
<tr>
<td>11</td>
<td>Appliance box fails to connect to the Chef server</td>
<td>Networking problems, configuration errors, etc.</td>
<td>Moderate</td>
<td>Small</td>
<td>Low</td>
<td>Yes</td>
<td>Can potentially be fixed by fixing the network problems or replacing the box</td>
</tr>
</tbody>
</table>

² https://docs.chef.io/chef_vault.html
## Appendix B. Prevention plan

<table>
<thead>
<tr>
<th>Threat ID</th>
<th>Threat / Unwanted incident</th>
<th>Risk level</th>
<th>Planned prevention measures</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.</td>
<td>Unauthorized remote access to Chef Server (&quot;root rights&quot;) (server encryption keys, public keys of all clients, IP addresses and configurations of all clients)</td>
<td>Low</td>
<td>SSH access restricted to machines on NSE network</td>
</tr>
<tr>
<td>5a.</td>
<td>Unauthorized remote access to SNOW-box through reverse SSH tunnel</td>
<td>Low</td>
<td>Relay virtual machine should be created for every use of reverse SSH tunnel and destroyed after use</td>
</tr>
</tbody>
</table>
Risikovurderingsrapport

SNOW appliance
Legekontor-PC

2.0
03.05.2016

Andrius Budrionis
Torje Henriksen
Johan Gustav Bellika
Joseph Stephen Hurley
Rune Hæta
Sammendrag

Bakgrunn for risikoanalysen
I løpet av våren 2015 satt Snow-prosjektet i gang et arbeid med å undersøke muligheten for å bruke dedikert maskinvare til tjenester som er utviklet av prosjektet, og som i dag er installert ute på legekontorene. Hensikten er å minimere risiko for forstyrrelser på EPJ-systemene ved at maskinvareressurser deles mellom EPJ og programvare som installeres i regi av prosjektet. Denne analysen forsøker å avdekke nye typer trusler som oppstår som en konsekvens av å benytte dedikert maskinvare.

Et møte ble avholdt første gang 28.04.2015, og deretter 05.05.2015, hvor trusselbilder, konsekvenser og risiko ble diskutert. Møtedeltakere: Torje Henriksen, Johan Gustav Bellika og Rune Hætta.

Risikoanalysen ble oppdatert 03.05.2016, hvor trusselbilder, konsekvenser og risiko ble diskutert og vurdert på nytt. Møtedeltakere: Andrius Budrionis, Torje Henriksen, Johan Gustav Bellika og Joseph Stephen Hurley.

Hovedkonklusjoner
Bruk av dedikert maskinvare til tjenester som utvikles i Snow-prosjektet minimerer risikoen for driftsforstyrrelser for installasjoner på legekontorene. Samtidig introduserer et separat system et behov for administrativ tilgang til de maskinene som utplasseres i løpet av en pilotperiode hvor tjenesten utvikles. Uautorisert tilgang til EPJ-data og til Snow-tjenester anses som de største truslene. Sikkerhetsbarrierene som er implementert er etter vår mening tilstrekkelig for en akseptabel risiko.
Innholdsfortegnelse

Sammendrag .................................................................................................................. 2
Bakgrunn for risikoanalysen ......................................................................................... 2
Hovedkonklusjoner ....................................................................................................... 2
1. System- og tjenestebeskrivelse .................................................................................. 4
   1.1. Om legekontor-PC ............................................................................................ 4
   1.2. Informasjon som behandles .............................................................................. 4
   1.3. Fjernkonfigurasjon ............................................................................................ 4
   1.4. Teknisk drift ..................................................................................................... 4
   1.5. Sikkerhetsmekanismer ...................................................................................... 5
2. Definisjon av sannsynlighet, konsekvens og risikonivå .............................................. 5
   2.1. Sannsynlighet ................................................................................................... 5
   2.2. Konsekvens ...................................................................................................... 5
   2.3. Om akseptkriterier ......................................................................................... 7
   2.4. Risikonivå ....................................................................................................... 7
3. Trusselidentifisering og –analyse .............................................................................. 8
   3.1. Uautorisert fysisk tilgang ................................................................................ 8
   3.2. Uautorisert fjerntilgang .................................................................................. 8
       3.2.1. Tap av passord og SSH-autentiseringsnøkler ........................................... 8
       3.2.2. Sikkerhetshull i SSH ............................................................................... 8
   3.3. Tjenestetopp .................................................................................................... 8
       3.3.1. Infrastruktur ............................................................................................ 8
       3.3.2. Maskinvarefeil ...................................................................................... 9
       3.3.3. Oppdateringsfeil .................................................................................... 9
   3.4. Uautorisert tilgang til personopplysninger i EPJ ............................................. 9
   3.5. Spredning av skadelig programvare ................................................................. 9
   3.6. Risikomatrise .................................................................................................. 9
4. Konklusjon og anbefalinger ..................................................................................... 10
Referanser .................................................................................................................... 10
Vedlegg A. Trusseltabell ............................................................................................... 11
Vedlegg B. Tiltaksplan .................................................................................................. 12
1. System- og tjenestebeskrivelse


1.1. Om legekontor-PC

Maskinvaren som benyttes er standard PC med noe redusert lagring – og prosesseringskapasitet sammenliknet med vanlige arbeidstasjoner. Den er relativt liten i størrelse, og skal enkelt kunne kobles på legekontorets interne LAN via nettkabel.

Det legges opp til at PC’en installeres ferdig med nødvendig operativsystem og programvare før den sendes ut til det aktuelle legekontoret.

PC’en har i tillegg en kortleser, basert på USB eller SD, som brukes til å lese ut data fra et medium som inneholder sertifikater og krypteringsnøkler.

Kun gitte personer i Snow-prosjektet og IT ansvarlige på legekontorer har tilgang til å logge inn på PC’en.

1.2. Informasjon som behandles


Agreggerte data brukes som grunnlag for en rapport som også genereres av legekontorserveren, dvs i PC’en. Først når rapporten er ferdig, sendes denne inn til et sentralt mottak utenfor legekontoret. Dette mottaket er en del av Snow-prosjektets infrastruktur.

1.3. Fjernkonfigurasjon

Chef server brukes for å konfigurere og oppdatere legekontorservere uten å kreve direkte fjerntilgang. Bruk av Chef er risikovurdert, identifiserte trusler er karakterisert som lave risikoer for systemet [1].

1.4. Teknisk drift

Snow-prosjektet har det tekniske driftsansvaret for alle utplasserte legekontor-PC-er. Konfigurasjonssystemet (beskrevet i forrige avsnitt) vil være en sentral del i driftsrutinene. Prosjektet har som mål å gjøre fjerntilgang overflødig ved hjelp av dette systemet. Så lenge serverløsningen er under utvikling, vil det være behov for administrativ fjerntilgang via reversert SSH tunnel (beskrevet og risikovurdert tidligere) [1].

[1] https://www.chef.io
Legekontors lokal IT driftsansvarlig får direkte tilgang til legekontor-PC med egen brukernavn og passord.

1.5. **Sikkerhetsmekanismer**

En rekke sikkerhetsmekanismer er implementert for å ivareta tilstrekkelig beskyttelse av involverte systemer. De viktigste er:

- SSH-basert innlogging sørger for sikret administrativ tilgang til legekontorserveren.
- Brannmurbeskyttelse som hindrer direkte fjernaksess.
- Alle tilkoblinger initieres fra legekontor-pc mot nettverk av lavere sikkerhetsnivå.
- Passordbeskyttet EPJ-tilgang fra serveren.
- Begrensede uttrekksmuligheter fra EPJ på grunn av ferdigdefinerte database-views.
- Et konfigurasjonssystem som reduserer behovet for direkte tilgang til legekontor-PC.
- Krypterte konfigurasjonsdata sikrer konfidensiellhet og autentisitet.
- Fysisk skille av kjøretidsmiljø. Bruk av dedikert maskinvare i er seg selv en løsning som bedre beskytter EPJ-systemet mot programvarefeil eller lignende i legekontorserveren.

Andre sikkerhetsmekanismer vurderes forløpende ved behov.

2. **Definisjon av sannsynlighet, konsekvens og risikonivå**

Vi velger å bruke kvalitative verdier for sannsynlighet, konsekvens og risikonivå.

2.1. **Sannsynlighet**

Vi har her valgt fire nivå for sannsynlighet – Høy, Middels, Liten og Svært Liten. Eksempler på definisjon av verdier for og beskrivelser av de ulike nivåene er vist i Tabellen 1. Eksemplerne er basert på felles mal utarbeidet av NST.

Tabell 1. Sannsynlighetskategorier med kriterier

<table>
<thead>
<tr>
<th>Sannsynlighet</th>
<th>Forventet frekvens</th>
<th>Nødvendige sikkerhets tiltak</th>
<th>Letthet Ressurser</th>
</tr>
</thead>
</table>

2.2. **Konsekvens**

Vi har valgt fire nivå for konsekvens – Liten, Moderat, Alvorlig og Katastrofal (Tabell 2). Kriteriene er hentet fra felles mal utarbeidet av NST.
<table>
<thead>
<tr>
<th>Konsevens</th>
<th>Lovregulering</th>
<th>Økonomi</th>
<th>Tilgjengelighet</th>
<th>Ressursbruk</th>
<th>Anseelse, rykte, tillit</th>
<th>Kvalitet på helsehjelp</th>
<th>Pasientenes personvern</th>
</tr>
</thead>
</table>
2.3. **Om akseptkriterier**

Eksempler på akseptkriterier som ligger til grunn for denne risikovurderingen er listet nedenfor. Vi legger til grunn at alle helseopplysninger relatert til en bestemt person er *sensitiv* informasjon (jf. Personopplysningsloven § 2 pkt 8c). Ingen andre enn de som har et behandlingsansvar for denne personen skal ha tilgang til helseinformasjonen.

Det er ikke akseptabelt:

- at sannsynligheten for at en pasient dør eller får varig helsetap som en følge av at denne tjenesten blir brukt er større enn sannsynligheten for at pasienten dør eller får varig helsetap hvis tjenesten ikke blir brukt
- at sannsynligheten for at uvedkommende får innsyn i (ser og hører) helseinformasjonen som overføres er større enn Svært liten.
- at sannsynligheten for at uvedkommende kan endre helseinformasjon under overføring er større enn Svært liten.
- at sannsynligheten for at legekontor-PC kan skape driftsforstyrrelser på EPJ-system er større enn Svært Liten

I risikomatrisen i neste avsnitt defineres hvilke kombinasjoner av sannsynlighet og konsekvens som ikke er akseptable (Tabell 3).

2.4. **Risikonivå**

Risikomatrisen viser risikonivået for hver trussel som kombinasjonen av truselens sannsynlighet og konsekvens. Vi har her valgt å bruke tre risikonivå: Lav, Middels og Høy (med ulike fargekoder).

<table>
<thead>
<tr>
<th>Tabell 3 Risikomatrise med risikonivå</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sannsynlighet:</td>
</tr>
<tr>
<td>Svært liten</td>
</tr>
<tr>
<td>Liten</td>
</tr>
<tr>
<td>Middels</td>
</tr>
<tr>
<td>Høy</td>
</tr>
</tbody>
</table>

Definerte risikonivå:

- **Lav risiko**: Trusler som har dette risikonivået aksepteres, men det bør rutinemessig vurderes om truslene endrer karakter og/eller bør følges nærmere opp. Åpenbare risikoreducerende tiltak vurderes.
- **Middels risiko**: Trusler som har dette risikonivået må det snarest innføres bedre rutiner for å håndtere, evt. må ytterligere analyse foretas. Tjenesten(e) kan etter vurdering fortsatt benyttes inntil risikoreducerende tiltak er iverksatt.
• **Høy risiko**: Ikke akseptabel risiko. Risikoreducerende tiltak må iverksettes før tjenesten kan benyttes videre, eventuelt må det gjøres midlertidige endringer som reduserer risikoen til middels risikonivå inntil tilstrekkelig sikkerhet er etablert.

### 3. Trusselidentifisering og –analyse

Her gis en kort beskrivelse av mulige trusselbilder og tilhørende årsaker og forutsetninger. Vedlegg A gir en oppsummering ved hjelp av en tabelloversikt.

#### 3.1. **Uautorisert fysisk tilgang**


#### 3.2. **Uautorisert fjerntilgang**


**3.2.1. Tap av passord og SSH-autentiseringsnøkler**

SSH-innlogging bygger på nøkkel-autentisering, som betyr at SSH-bruker må både ha tilgang til gyldige autentiseringsnøkler og passord for å låse disse opp. Passord er personlig for hvert enkelt bruker som trenger tilgang, mens nøklene lagres og lesebeskyttes på dedikerte systemer som kontrolleres av Snow-prosjektet.

**3.2.2. Sikkerhetshull i SSH**


#### 3.3. **Tjenestestopp**

Tjenestestopp innebærer at legekontorserveren av en eller annen grunn svikter.

**3.3.1. Infrastruktur**

Feil i infrastruktur innebefatter strømbrudd, nettbrudd, og annet liknende som er en forutsetning for at tjenesten skal kunne fungere. Strømbrudd skal normalt ikke gi varige skader på maskinen, men det kan oppstå behov for å måtte slå den på igjen når strømmen er tilbake, noe det forutsettes at legekontoret selv kan bistå med. Et eventuelt nettbrudd vil skape problemer med kommunikasjonen mellom PC, EPJ-system og Snow-infrastrukturen. Det forutsettes at infrastrukturen har en noenlunde normal oppetid, og at ansvaret for dette er noe legekontorene har selv.
3.3.2. Maskinvarefeil

3.3.3. Oppdateringsfeil

3.4. Uautorisert tilgang til personopplysninger i EPJ
Legekontor-PC’en er installert med programvare som gjør det mulig å trekke data ut fra lokale EPJ-systemer. Potensialet er dermed til stedet for å få tilgang til personopplysninger som ligger lagret i EPJ. Forutsetningen er at det allerede er en uautorisert tilgang til legekontor-PC’en (ref. 3.1 og 3.2). I tillegg kreves brukernavn og passord for å kunne kjøre database-spørringer mot selve EPJ-systemet.

3.5. Spredning av skadelig programvare
Skadelig programvare er her underforstått datavirus, trojanere, ormer og lignende, som kan spre seg til flere systemer, ødelegge data og sette eksisterende system ut av funksjon. Slik programvare har som regel ukjent opphav, og er først og fremst et problem i miljø hvor sluttbrukere har tilgang til å installere eller hente inn programvare. Det beste forsvaret mot skadelig programvare er derfor å sørge for at programvare alltid kommer i fra kjente kilder.

Snow-prosjektet benytter programvare fra en rekke eksterne aktører. Siden prosjektet i stor grad bygger sine systemer ved hjelp av fri programvare, vil kildekode i de fleste tilfeller være fritt tilgjengelig for gjennomgang. Ferdigkompilerte programvarepakker er i tillegg tilgjengeliggjort av flere distributører. Slike pakker signeres gjerne slik at installasjonsverktøyene kan verifisere opphavet.

3.6. Risikomatriese
Trusseltabellen i vedlegg A summerer opp de trusslene prosjektet har identifisert med tilhørende vurdering for sannsynlighet, konsekvens og risiko. Tabell 4 viser de identifiserte truslene sammen med risikonivåer.

<table>
<thead>
<tr>
<th>Konsekvens:</th>
<th>Sannsynlighet:</th>
<th>Sannsynlighet:</th>
<th>Alvorlig</th>
<th>Katastrofal</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Liten</td>
<td>Moderat</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Svært liten</td>
<td>2.2., 3.2., 3.3.</td>
<td>5.</td>
<td>2.1., 4.</td>
<td></td>
</tr>
<tr>
<td>Liten</td>
<td>1.</td>
<td>3.1.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Middels</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Høy</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
4. Konklusjon og anbefalinger
Snow-prosjektet har identifisert et sett med trusler knyttet til bruk av dedikert maskinvare som legekontorserver. Bruk av dedikert maskinvare innebærer at legekontorserveren kjører på et selvstendig system som administreres av prosjektet. Slik administrasjon er vanskelig å få til uten en eller annen form for fjernaksess.

Fjernaksess øker imidlertid risikoen for uautorisert tilgang til systemer ved legekontorene hvor pasientopplysninger lagres. Prosjektet har derfor som strategisk mål å ta i bruk et konfigurasjonssystem som i størst mulig grad reduserer behovet for fjerntilgang. Konfigurasjonssystemet og fjerntilgang løsningen er beskrevet og risikovurdert tidligere [1].

Referanser

### Vedlegg A. Trusseltabell

<table>
<thead>
<tr>
<th>ID</th>
<th>Trussel / Kompromittering</th>
<th>Årsak</th>
<th>Sannsynlighet</th>
<th>Konsekvens</th>
<th>Risiko</th>
<th>Akseptabel risiko</th>
<th>Kommentarer og beskrivelse av implementerte tiltak</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Uautorisert fysisk tilgang</td>
<td>Tyvert, mistet, innbrudd</td>
<td>Liten</td>
<td>Liten</td>
<td>Lav</td>
<td>Ja</td>
<td>Antar begrenset tilgang tilsvarende EPJ-system. Kan få tilgang til export-programvare. Bare pseudonymiserte data lagres på fastlegekontor-pc.</td>
</tr>
<tr>
<td>2.1</td>
<td>Uautorisert fjerntilgang</td>
<td>Tap av passord og SSH-nøkler (Chef server, legekontor-pc, relay server)</td>
<td>Svært liten</td>
<td>Alvorlig</td>
<td>Lav</td>
<td>Ja</td>
<td>Krav om nøkkelbasert autentisering. Direkte fjerntilgang finnes ikke, flere servere må kompromiseres samtidig. SSH tunnel er opprettet &quot;on demand&quot; og fjernet etter bruk. SSH tunnel sesjon utløper hvis den er ikke i bruk.</td>
</tr>
<tr>
<td>2.2</td>
<td></td>
<td>Sikkerhetshull i SSH</td>
<td>Liten</td>
<td>Liten</td>
<td>Lav</td>
<td>Ja</td>
<td>Historisk sett liten sannsynlighet. Sikkerhetsoppdateringer skjer automatisk</td>
</tr>
<tr>
<td>3.1</td>
<td>Tjenestestopp</td>
<td>Infrastrukturfeil (strøm, nett, etc…)</td>
<td>Moderat</td>
<td>Liten</td>
<td>Lav</td>
<td>Ja</td>
<td>Maskin må slås på automatisk, re-etablere nettforbindelser</td>
</tr>
<tr>
<td>3.2</td>
<td></td>
<td>Maskinvarefeil</td>
<td>Svært liten</td>
<td>Liten</td>
<td>Lav</td>
<td>Ja</td>
<td></td>
</tr>
<tr>
<td>3.3</td>
<td></td>
<td>Oppdateringsfeil</td>
<td>Svært liten</td>
<td>Liten (Alvorlig for prosjektet)</td>
<td>Lav</td>
<td>Ja (Nei)</td>
<td>Automatisk oppdatering påslått</td>
</tr>
<tr>
<td>4</td>
<td>Uautorisert tilgang til personopplysninger (i EPJ)</td>
<td>Tilgang til klientmaskin, tap av passord og SSH-nøkler, og tap av passord til EPJ</td>
<td>Svært liten</td>
<td>Alvorlig</td>
<td>Lav</td>
<td>Ja</td>
<td>Inkluderer tiltak fra 2.1. og 2.2. Begrensninger i EPJ uttrykksmuligheter.</td>
</tr>
<tr>
<td>5</td>
<td></td>
<td>Import av programvare fra eksterne kilder</td>
<td>Svært Liten</td>
<td>Moderat</td>
<td>Lav</td>
<td>Ja</td>
<td>Programvare hentes kun fra autentiserte og kjente kilder, og eksekverer med moderate rettigheter.</td>
</tr>
</tbody>
</table>
### Vedlegg B. Tiltaksplan

<table>
<thead>
<tr>
<th>ID</th>
<th>Uakseptabel trussel</th>
<th>Tiltak</th>
<th>Ansvarlig</th>
<th>Frist</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1.</td>
<td>Uautorisert fjerntilgang</td>
<td>Innlogging kun mulig fra spesifiserte maskiner med begrenset tilgang&lt;br&gt;Prosedyrer for distribusjon av passord og SSH nøkler til IT ansvarlige på legekontorer er dokumentert på SNOW wiki. Overleveringen er i samsvar med etablert praksis (post, digipost)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
ROS-vurdering

Installasjon av SNOW-server i HMN

Rapporten inneholder:
  Oppsummering
  Forutsetninger og avgrensinger
  Beskrivelse av analyseobjekt
    Anbefaling
    Beslutning
  Vedlegg: Hendelser

26.08.2016
Innhold
1. Oppsummering .................................................................................................................. 3
2. Forutsetninger og avgrensinger .......................................................................................... 4
3. Beskrivelse av analyseobjekt .............................................................................................. 4
4. Eksisterende tiltak ................................................................................................................. 7
5. Nye tiltak ................................................................................................................................ 8
Vedlegg A: Hendelser .............................................................................................................. 10
1. Oppsummering

Denne risikovurderingen er gjennomført med den informasjonen som var tilgjengelig på analysetidspunktet. Den er gjennomført av ressurer fra Forvaltning, Virksomhetsutvikling og Telemed (Nasjonalt senter for e-helseforskning).

Hovedfunnene tilsier at det er lav risiko forbundet med installasjon av en SNOW-server i HMN.

Det er knyttet størst risiko til påvirkning av HMN produksjonsmiljø som følge av automatiske programvareoppdateringer av SNOW-server. De viktigste tiltakene er herding og nedlåsning av tilganger for SNOW-server.

For de resterende hendelsene er det lav risiko, og eksisterende tiltak ansees som tilstrekkelige. Det ble allikevel identifisert 4 nye tiltak som kan bidra til å senke risikoen ytterligere. Tiltakene omhandler sikring av server og rutiner ved Lab, disse er beskrevet nærmere for den enkelte hendelsen.

Deltakere:

<table>
<thead>
<tr>
<th>Del-takernr.</th>
<th>Navn</th>
<th>Funksjon</th>
<th>Virksomhet</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Ørnulf Landfald</td>
<td>Oppdragsansvarlig</td>
<td>Hemit</td>
</tr>
<tr>
<td>2</td>
<td>Geir Reset Simonsen</td>
<td>Rådgiver infrastruktur</td>
<td>Hemit</td>
</tr>
<tr>
<td>3</td>
<td>Torje Henriksen</td>
<td>Systemutvikler</td>
<td>Telemed</td>
</tr>
<tr>
<td>4</td>
<td>Åsmund K Lie</td>
<td>ROS-tilrettelegger</td>
<td>Hemit</td>
</tr>
</tbody>
</table>

Tidsplan og aktivitet:

<table>
<thead>
<tr>
<th>Aktivitet</th>
<th>Dato</th>
<th>Deltakernr.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oppstart</td>
<td>13.06.16</td>
<td>1, 4</td>
</tr>
<tr>
<td>Utarbeidet hendelsesliste</td>
<td>23.06.16</td>
<td>1, 2, 3, 4</td>
</tr>
<tr>
<td>Møte risikovurdering I</td>
<td>23.06.16</td>
<td>1, 2, 3, 4</td>
</tr>
<tr>
<td>Utarbeidet utkast til rapport</td>
<td>24.06.16</td>
<td>4</td>
</tr>
</tbody>
</table>
2. Forutsetninger og avgrensinger

Forutsetninger
Denne risikovurderingen forutsetter at SNOW-tjenesten fungerer slik den er tiltenkt, kun med pseudonymiserte og anonymiserte data.

Når det gjelder drift av SNOW serveren så skal den inn i standard regime for serverdrift i sikker sone. Det samme gjelder for tilgang utenfra til serveren.

Risikovurderingen dekker
- SNOW-server på St. Olav
- Kommunikasjon mellom lab-system og SNOW-server
- Kommunikasjon mellom SNOW-server og SNOW kommunikasjonssentral

Risikovurderingen dekker ikke
- Tjenester som bygges på bakgrunn av data som kommer ut fra SNOW-server

3. Beskrivelse av analyseobjekt
SNOW er en løsning for symptombasert sykdomsovervåkning i Norge. Løsningen benytter deling av epidemiologiske data mellom pasienter, primærleger, mikrobiologi-laboratorieleger for å forebygge og behandle smittsomme sykdommer. SNOW skal bidra til:

1. Tidligere varsling av epidemier
2. Tidligere diagnostisering og intervención
3. Lavere antall smittede
4. Reduserte kostnader forbundet med utbrudd av smittsomme sykdommer

I HMN er det planlagt installasjon av en SNOW-server på St. Olav som skal videreformidle anonymiserte data til SNOW koordineringstjener i Helsenettet.

Personopplysning i system
SNOW-tjenesten inneholder ikke direkte identifiserbare helseopplysninger:
• Data mellom lab- og SNOW er pseudonymisert
• Data som går ut av SNOW-server er anonymisert
  o Fylkesnivå - uke, kjønn, alder
  o Kommunenivå - måned, kjønn, alder

Arbeidsflyt
Ikke relevant.

Konfigurasjonskart for teknisk løsning
SNOW-server aggregerer data før det sendes ut til SNOW koordineringstjener:

Tabellen under beskriver hvilke porter som må åpnes mellom SNOW lokal tjener og koordineringstjener for at tjenesten skal virke tilfredsstillende.

• Den lister åpningene som må gjøres.
• Det forventes at trafikk får flyte begge veier på allerede etablerte forbindelser.

<table>
<thead>
<tr>
<th>Kilde</th>
<th>Destinasjon</th>
<th>Port</th>
<th>Protokoll</th>
<th>Bruk</th>
<th>Hemit Merknad</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lokal SNOW-tjener</td>
<td>Koordinator/ po1.snow.nhn.no</td>
<td>Tcp/80</td>
<td>http</td>
<td>Polling etter programvareoppdateringer.</td>
<td>Hemit åpner for utgående trafikk fra Lokal SNOW-</td>
</tr>
<tr>
<td>Lokal SNOW-tjener</td>
<td>Koordinator/koordinator.po1.snow.nhn.no</td>
<td>Tcp/443</td>
<td>https</td>
<td>Samme som for http</td>
<td>Hemit åpner for utgående trafikk fra Lokal SNOW-tjener på Tcp/443</td>
</tr>
<tr>
<td>-------------------</td>
<td>----------------------------------------</td>
<td>--------</td>
<td>-------</td>
<td>-------------------</td>
<td>---------------------------------------------------------------</td>
</tr>
<tr>
<td>Lokal SNOW-tjener</td>
<td>Koordinator/koordinator.po1.snow.nhn.no</td>
<td>Tcp/5269</td>
<td>XMPP S2S</td>
<td>Mer eller mindre konstant forbindelse som brukes for å sende XMPP meldinger mellom tjenerne.</td>
<td>Hemit åpner for utgående trafikk fra Lokal SNOW-tjener på Tcp/5269</td>
</tr>
<tr>
<td>Lab-system</td>
<td>Lokal SNOW-tjener</td>
<td></td>
<td></td>
<td>SSIS pakke som trekker ut data fra Lab-miljøet og som skriver dette til en CSV fil som lagres på SNOW tjener</td>
<td></td>
</tr>
</tbody>
</table>

**Rutiner og opplæring**

Ikke relevant.
4. Risiko og eksisterende tiltak

4.1. SNOW-server påvirker HMN produksjonsmiljø

4.2. Utenforstående får tilgang via SNOW DB/Lab-server

4.3. Uautorisert tilgang til pseudonymiserte data i sikker sone

<table>
<thead>
<tr>
<th>Eksisterende tiltak</th>
<th>Status</th>
<th>Investering</th>
<th>Kostnad pr. år</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database satt opp for ikke å kommunisere på nettet</td>
<td>Besluttet</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

4.4. Lab-analyser blir ikke eksportert til SNOW-server

4.5. ROS-matrise - Nå-situasjon

4.5.1. Alle konsekvensområder

<table>
<thead>
<tr>
<th></th>
<th>Ubetydelig 1</th>
<th>Moderat 2</th>
<th>Betydelig 3</th>
<th>Alvorlig 4</th>
<th>Kritisk 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Meget sannsynlig</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>5</td>
</tr>
<tr>
<td>Sannsynlig</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td>4</td>
</tr>
<tr>
<td>Mulig</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>Mindre sannsynlig</td>
<td>2</td>
<td>1</td>
<td></td>
<td></td>
<td>2</td>
</tr>
<tr>
<td>Usannsynlig</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

4.5.1.1. Tiltak må iverksettes
- Ingen hendelser

4.5.1.2. Tiltak bør iverksettes
- 1 SNOW-server påvirker HMN produksjonsmiljø (D2)
4.5.1.3. Kan aksepteres
- 2 Utenforstående får tilgang via SNOW DB/Lab-server (C2)
- 3 Uautorisert tilgang til pseudonymiserte data i sikker sone (C2)
- 4 Lab-analyser blir ikke eksportert til SNOW-server (A4)

5. Risiko og nye tiltak

5.1. 1 SNOW-server påvirker HMN produksjonsmiljø

<table>
<thead>
<tr>
<th>Nye tiltak</th>
<th>Status</th>
<th>Investering</th>
<th>Kostnad pr. år</th>
</tr>
</thead>
<tbody>
<tr>
<td>Herding av SNOW-server</td>
<td>Anbefalt</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Stenge for andre tilganger enn de som kreves for å opprettholde tjenesten</td>
<td>Anbefalt</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

5.2. 2 Utenforstående får tilgang via SNOW DB/Lab-server

<table>
<thead>
<tr>
<th>Nye tiltak</th>
<th>Status</th>
<th>Investering</th>
<th>Kostnad pr. år</th>
</tr>
</thead>
<tbody>
<tr>
<td>Konfigurere slik at XMPP ikke lytter på port 5269</td>
<td>Anbefalt</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

5.3. 3 Uautorisert tilgang til pseudonymiserte data i sikker sone

<table>
<thead>
<tr>
<th>Nye tiltak</th>
<th>Status</th>
<th>Investering</th>
<th>Kostnad pr. år</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sikre fil-share (begrenset lesetilgang)</td>
<td>Anbefalt</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

5.4. 4 Lab-analyser blir ikke eksportert til SNOW-server

<table>
<thead>
<tr>
<th>Nye tiltak</th>
<th>Status</th>
<th>Investering</th>
<th>Kostnad pr. år</th>
</tr>
</thead>
<tbody>
<tr>
<td>Innarbeide rutiner for Lab</td>
<td>Anbefalt</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Leverandør (SNOW) må monitorere rapporteringen</td>
<td>Anbefalt</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
5.5. ROS-matrise - Rest-risiko

5.5.1. Alle konsekvensområder

<table>
<thead>
<tr>
<th></th>
<th>Ubetydelig 1</th>
<th>Moderat 2</th>
<th>Betydelig 3</th>
<th>Alvorlig 4</th>
<th>Kritisk 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>Meget sannsynlig</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>5</td>
</tr>
<tr>
<td>Sannsynlig</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4</td>
</tr>
<tr>
<td>Mulig</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>Mindre sannsynlig</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>2</td>
</tr>
<tr>
<td>Usannsynlig</td>
<td>2 1</td>
<td></td>
<td></td>
<td></td>
<td>1</td>
</tr>
</tbody>
</table>

5.5.1.1. Tiltak må iverksettes
- *Ingen hendelser*

5.5.1.2. Tiltak bør iverksettes
- *Ingen hendelser*

5.5.1.3. Kan aksepteres
- 1 SNOW-server påvirker HMN produksjonsmiljø (D1)
- 2 Utenforstående får tilgang via SNOW DB/Lab-server (C1)
- 3 Uautorisert tilgang til pseudonymiserte data i sikker sone (C1)
- 4 Lab-analyser blir ikke eksportert til SNOW-server (A3)
### Vedlegg A: Hendelser

**Hendelse: 1 SNOW-server påvirker HMN produksjonsmiljø**

<table>
<thead>
<tr>
<th></th>
<th>Nå-situasjon:</th>
<th>Rest-risiko:</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Sannsynlighetsgrad:</strong></td>
<td>Mindre sannsynlig</td>
<td>Usannsynlig</td>
</tr>
<tr>
<td><strong>Konsekvensgrad:</strong></td>
<td>Alvorlig 4</td>
<td>Alvorlig 4</td>
</tr>
</tbody>
</table>

#### Årsaker

<table>
<thead>
<tr>
<th>Årsaker</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Snow-serveren oppdateres automatisk med programvare utenfra</td>
<td></td>
</tr>
</tbody>
</table>

#### Konsekvenser

<table>
<thead>
<tr>
<th>Konsekvenser</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Driftsforstyrrelser (Konfidensialitet)</td>
<td></td>
</tr>
</tbody>
</table>

#### Eksisterende tiltak

<table>
<thead>
<tr>
<th>Eksisterende tiltak</th>
<th>Status</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Herding av SNOW-server</td>
<td>Anbefalt</td>
<td>Forebyggende</td>
</tr>
<tr>
<td>Stenge for andre tilganger enn de som kreves for å opprettholde tjenesten</td>
<td>Anbefalt</td>
<td>Forebyggende</td>
</tr>
</tbody>
</table>

#### Nye tiltak

<table>
<thead>
<tr>
<th>Nye tiltak</th>
<th>Status</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Herding av SNOW-server</td>
<td>Anbefalt</td>
<td>Forebyggende</td>
</tr>
<tr>
<td>Stenge for andre tilganger enn de som kreves for å opprettholde tjenesten</td>
<td>Anbefalt</td>
<td>Forebyggende</td>
</tr>
</tbody>
</table>
### Årsaker
- Sikkerhetshull i XMPP
- SQL-injection

### Konsekvenser
- Uautorisert innsyn i person- og/eller helseopplysninger (Konfidensialitet)

### Eksisterende tiltak

<table>
<thead>
<tr>
<th>Årsaker</th>
<th>Status</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sikkerhetshull i XMPP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SQL-injection</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Nye tiltak

<table>
<thead>
<tr>
<th>Nye tiltak</th>
<th>Status</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Konfigurere slik at XMPP ikke lytter på port 5269</td>
<td>Anbefalt</td>
<td>Forebyggende</td>
</tr>
</tbody>
</table>
Hendelse: 3 Uautorisert tilgang til pseudonymiserte data i sikker sone

<table>
<thead>
<tr>
<th>Beskrivelse:</th>
</tr>
</thead>
</table>
| • Fra SNOW DB  
| • Eksport-filer fra labsystem |

<table>
<thead>
<tr>
<th>Nå-situasjon:</th>
<th>Rest-risiko:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sannsynlighetsgrad:</td>
<td>Mindre sannsynlig</td>
</tr>
<tr>
<td>Konsekvensgrad:</td>
<td>Betydelig 3</td>
</tr>
</tbody>
</table>

**Årsaker**

- Uautorisert tilgang til databasen
- Uautorisert tilgang til fil-share

**Konsekvenser**

- Data i eksport-filer manipuleres (Integritet)
- Helseopplysninger kommer på avveie (Konfidensialitet)

**Eksisterende tiltak**

| Status | Type  
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Database satt opp for ikke å kommunisere på nettet</td>
<td>Besluttet</td>
</tr>
</tbody>
</table>

**Nye tiltak**

| Status | Type  
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Sikre fil-share (begrenset lesetilgang)</td>
<td>Anbefalt</td>
</tr>
</tbody>
</table>
Hendelse: 4 Lab-analyser blir ikke eksportert til SNOW-server

<table>
<thead>
<tr>
<th></th>
<th>Nå-situasjon:</th>
<th>Rest-risiko:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sannsynlighetsgrad:</td>
<td>Sannsynlig</td>
<td>Mulig</td>
</tr>
<tr>
<td>Konsevensgrad:</td>
<td>Ubetydelig 1</td>
<td>Ubetydelig 1</td>
</tr>
</tbody>
</table>

Årsaker

Nye lab-koder

Konsekvenser

Feil rapporter (Integritet)

Eksisterende tiltak

Eksisterende tiltak | Status | Type
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Innarbeide rutiner for Lab</td>
<td>Anbefalt</td>
<td>Forebyggende</td>
</tr>
<tr>
<td>Leverandør (SNOW) må monitorere rapporteringen</td>
<td>Anbefalt</td>
<td>Begrensende</td>
</tr>
</tbody>
</table>

Nye tiltak

Nye tiltak | Status | Type
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Innarbeide rutiner for Lab</td>
<td>Anbefalt</td>
<td>Forebyggende</td>
</tr>
<tr>
<td>Leverandør (SNOW) må monitorere rapporteringen</td>
<td>Anbefalt</td>
<td>Begrensende</td>
</tr>
</tbody>
</table>