1 Definition of likelihood, consequence and risk levels

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

1.1 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 1: Definition of likelihood levels

Likelihood	Frequency	Ease of misuse and motivation
Very high	Very often, occurs more often than every 10^{th} connection, i.e. more frequently than 10 % of the time/cases.	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.
High	Quite often. Occurs between 1 % and 10 % of the time/cases.	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.
Moderate	May happen. Occurs between 0.1 % and 1 % of the time/cases.	Normal knowledge about the system is sufficient; or normally available equipment can be used; or it can be performed deliberately.
Low	Rare. Occurs less than 0.1 % of the time/cases.	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.

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 [1]

Consequence:	
Small	For the patient: No impact on health; or negligible economic loss which can be restored; or small reduction of reputation in the short run. 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.
Moderate	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). 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.
Severe	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. 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.
Catastrophic	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. 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.

1.2 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.

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

It is not acceptable that[2]:

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 **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.)*

[1] These are the same four consequence levels as used by Helse Nord in their template for risk assessments.

[2] The letter in parenthesis refers to the security aspects confidentiality (C), integrity (I), availability (A)

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.)*

1.3 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 (table 4). 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

Risk level:	
Low	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.
Medium	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.
High	Not acceptable risk. Can not start using the service before risk reducing treatment has been implemented.

Table 4: Risk matrix showing the defined risk levels

Consequence: **Likelihood:**	**Small**	**Moderate**	**Severe**	**Catastrophic**
Low	Low	Low	Low	Medium
Moderate	Low	Medium	Medium	High
High	Low	Medium	High	High
Very high	Medium	High	High	High