Ledningsnätverket för Medicinsk Teknik
The Swedish Management Network for Biomedical Engineering

Inquiry

The Swedish Patient Data Act in the clinical everyday

- What demands are made on medical devices?

Condensed Report Part 2:
Application of information security
in medical devices and systems

30 September 2016
English version 23 October 2017

Summary

The Swedish Management Network for Biomedical Engineering ("Ledningsnätverket för Medicinsk Teknik," LfMT, www.lfmt.se) is the common forum for Swedish medical care mandators within the area of medical devices (MD). LfMT is part of the Swedish Association of Local Authorities and Regions, SALAR (SKL).

With the aim to inquire into and make proposals on management of medical devices (MD), taking into account the current conflict between the non-harmonized Swedish legislation on processing patient data (the Patient Data Act, "*Patientdatalagen,*" PDL) and the Swedish implementation of the EU directive concerning medical devices (the Medical Devices Act, "*Lagen om medicintekniska produkter,*" LMP), LfMT in 2014 appointed a working team consisting of members from its sub-network of System Integrators ("*SI-nätverket*"). The results of this team's efforts were presented in 2015 in the report "*The Swedish Patient Data Act in the clinical everyday - What demands are made on medical devices?"* (Hereafter referred to as "*Part 1*"). This report was widely disseminated and its conclusions were considered an interesting and good initiative among most actors in the medical care area in Sweden. The Swedish Data Protection Authority was essentially the only actor representing an opposing point of view.

This subsequent report is a condensed version of the original report (43 pages) in Swedish, referred to as "Part 2," and consists of two main sections:

I) Presenting the response to Part 1. The general opinion in the response to Part 1 has been that it is important to achieve a balance between the demand for activities to protect the integrity of the individual and the demand for essential protection of life and health. There are unfortunately no guiding principles from Swedish authorities concerning how to behave in practice in aiming to achieve a good balance in the mutual protection of these two values. LfMT has, in its dialogue with various Swedish authorities and other actors in this area, been informed that these entities will strive to secure both values in so far as possible.

II) Dealing with the main purpose of this report. The purpose is to test and show how the information concept "*MD data*," defined in Part 1, could be used to bridge the non-harmonized legislation concerning processing of patient data (PDL) and the Swedish implementation of the EU directive concerning medical devices (LMP). Section II also presents the results of a literature review and proposals for concrete guidelines and recommendations to actors in the MD area.

The fundamental stance of LfMT is that the benefits from use of MD should be greater than the risk that the patient is exposed to. In the report, LfMT suggests a model for balancing the protection of life and health and the protection of patient integrity, based on time criteria. These time criteria should be used as guidelines for the maximum time permissible for removing obstructions to *MD data* access. An example of this is given in the report.

The report concludes with recommendations from LfMT concerning the various problems previously discussed, and proposals for the continued work in this field. LfMT also concretizes which specific demands manufacturers and caregivers ought to manage independently and which should be managed in cooperation. LfMT recommends that the Swedish authorities the National Board of Health and Welfare ("*Socialstyrelsen,"* SoS), the Health and Social Care Inspectorate (*"Inspektionen för vård och omsorg,*" IVO) and the Medical Products Agency (*"Läkemedelsverket,"* LV) publish clear instructions addressed to all actors in the MD area, concerning the processing and review of *MD data* on the path from the patient to the medical chart.

Healthcare organizations process a huge volume of *MD data* daily. Pending an alteration of the Swedish legislation on patient data, LfMT recommends use of the Swedish implementation (the Personal Data Act, *"Personuppgiftslagen,"* PUL) of the EU directive 95/46/EG on the protection of personal data when processing *MD data.* Many of the actors in the healthcare area and a number of legal experts we have consulted with find this recommendation interesting, and suggest that it should be developed further by LfMT. This report is an attempt to elaborate LfMT's point of view. It is also intended to support processing of patient information from MDs, *MD data*, in the clinical environment, in accordance with the intentions of the Swedish legislative framework in PDL and PUL.

Terminology

Term	Explanation
DI	The Swedish Data Protection Authority, Datainspektionen
eHM	The Swedish eHealth Agency, eHälsomyndigheten
IVO	The Health and Social Care Inspectorate, Inspektionen för Vård och Omsorg
LfMT	The Swedish Management Network for Biomedical Technology, Ledningsnätverket för Medicinsk Teknik
LMP	The Medical Devices Act, Lagen om medicintekniska produkter (SOSFS 1993:584)
LV	The Medical Products Agency, Läkemedelsverket
MDR	The Medical Devices Regulation (EU) 2017/745
PDL	The Patient Data Act, Patientdatalagen (SOSFS 2008:355)
PSL	The Patient Safety Act, Patientsäkerhetslagen (SOSFS 2010:659)
PUL	The Personal Data Act, Personuppgiftslagen (SOSFS 1998:204)
SKL	The Swedish Association of Local Authorities and Regions (SALAR), Sveriges Kommuner och Landsting
SoS	The National Board of Health and Welfare, Socialstyrelsen

Part 1

Response to LfMT's report Part 1

The following problem description in our report Part 1 has been confirmed by a number of Swedish organizations and authorities. In brief, the problem relates to the fact that the legislative works PDL, LMP and PSL do not correlate with each other and do not even reference each other. The regulation on medical devices contains little information or guidance on how to design integrity-protecting measures. PDL, on its part, is designed to protect information in medical charts, but is interpreted by some to encompass all information generated by medical devices as well, irrespective of how the authenticity thereof has been assessed and confirmed. PSL states clearly that a patient has a right to safe healthcare.

Taken as a whole, this leads to vague requirements on traditional implementations of medical devices, which individual manufacturers can find difficult to manage. International medical device manufacturers see obvious difficulties in adapting their products based on PDL. Within clinical practice, there are also difficulties in managing the occasionally contradictory requirements of PDL and LMP. There is therefore a great need to identify where the limits are for when information from medical devices should be seen as a matter of medical record, which falls under PDL. Measures to safeguard information security must be included in risk management, so that they do not entail yet another source of danger to a patient's life or health.

In Part 1, LfMT suggested and defined a new information concept, *MD data*, which is central for the reasoning in this report:

> *"MD data" is information technologically generated (gathered and/or processed) through medical devices, in the form of biological (i.e., anatomical, physiological, chemical, microbiological, etc.) measurements and/or images from a patient (i.e., personal data in the form of measurements), which have not yet been assessed by certified medical staff as authentic and relevant for diagnosis or care of the patient and as such must be entered into the patient's medical chart.*

For "everyday use" the definition can be summed up as:

> *"MD data" is information from medical devices that has not yet been entered into a medical chart.*
> *MD data that has been entered into a medical chart is referred to as a "test result."*

The problem dealt with in the report can be said to encompass four areas:

1. The extent to which design of information security and authorization control negatively impacts upon efficiency in healthcare and thus entails a risk of physical harm to patients either through erroneous diagnosis and treatment or through failure to take medically necessary measures.

2. The extent to which flaws in the design of information security as regards authorization control contribute to intentional or accidental dissemination of patients' personal data, so that the privacy of patients is harmed.

3. The extent to which MD manufacturers are liable to, in their risk management processes, balance and safeguard the protection that each patient can rightfully expect against physical harm and against breaches of privacy.

4. The extent to which authorities can clarify the regulations on *MD data* on the path from registration of biological parameters in a patient to being entered as test results in a medical chart.

One of our conclusions is that there are differences of opinion separating the Swedish Data Protection Authority (DI) and healthcare authorities as regards these matters. The problem can, at the authority level, be worded as follows:

> How can authorities that protect differing special interests (DI, LV, SoS, IVO and eHM) come to an agreement, so that they jointly and proactively guide healthcare organizations and MD manufacturers as regards management of privacy matters in everyday practical use of MDs in healthcare?

It is very important that MDs also protect the privacy of patients, but that this is in balance with the assurance of physical safety for patients.

Part 2

Guidelines and recommendations to actors in the field

Objective

This report does not claim to give sufficient answers to all four of the aforementioned problem areas from Part 1. However, the objective is to provide a certain clarity and make suggestions on tangible solutions regarding some of the questions raised. We hope that this will lead to an increased understanding among the various actors in the field of the problems that LfMT has experienced in regard to application of the existing regulations. We hope that the affected parties, using our reports, will have the foundations for initiatives such as collaborations, reaching consensus and making improvements regarding the design and management of information security in MDs.

Information in medical charts should be relevant. It is the task of the person entering information into the chart to assess the relevance of *MD data* and if it should be included in the chart or not. Over-documentation in a patient chart also entails a risk for patient safety. When *MD data* becomes a test result in a chart, it must be stored for at least ten years under PDL.

PUL gives relevant guidance on the processing of *MD data*, including a statement in Section 9h that requires blocking or erasure of artefacts, i.e., such personal data (in this case *MD data*) as is incorrect and/or incomplete, and in Section 9i that *MD data* shall be destroyed when it is no longer needed. Healthcare organizations process very large volumes of *MD data* on a daily basis. Pending the revision of PDL, LfMT recommends that PUL is used as a guideline for the processing of *MD data*. This is a recommendation that many of the actors in healthcare and some legal scholars have found interesting and feel should be developed further. This report, Part 2, is an expansion of the view underlying that recommendation. Part 2 can also serve as support in observing PDL to a reasonable extent in processing *MD data*.

Literature review on information security and MD

In connection with the creation of this report, a literature review was performed in PubMed. This review has served to identify relevant publications in the field of MD and information security. Articles published between 2005 and 2015 were included.
The conclusions of the literature review are that:

- MDs connected to IT systems contain sensitive personal data.
- Such personal data must be protected if healthcare institutions are to retain the public's trust.
- MDs connected to IT networks must be protected under principles similar to those used for connected personal computers.
- Information security, in patient care, should be designed so that authorized healthcare personnel gets ”access to the information required, as and when needed.”
- If access is not possible through the normal route, there should be an alternative way to get emergency access to the information.
- More research and development is needed on how patient integrity and security should be managed.

We found no experience-based articles on integrity protection in MDs and the effects thereof on healthcare organizations or consequences regarding protection of life and health and protection of patient integrity for patients directly or indirectly connected to MDs.

General guidelines

Security of medical devices

According to the EU directive concerning medical devices (MDD) and the manufacturer's information, a MD is intended for a specific medical use. It should be clinically proven to have clinical benefits reflecting the medical use intended by the manufacturer (*intended use*). A MD should be suitable and satisfy the performance criteria drawn up by the manufacturer. For a regulatory standpoint, a MD should satisfy *vital requirements* on secure and appropriate technology that fulfils the criteria regarding protection of life and health. The clinical proof is weighed against the risk of harming the patient in a cost-benefit analysis. The benefit should greatly exceed the risk to which the patient is exposed. MDD clearly states that MD should be equipped to ”significantly protect life and health.”

Patient safety

The patient is, through PSL, granted the right to safe healthcare. The care provider has a duty and an organizational responsibility to, through management systems, perform systematic patient safety work regarding risk management and self-evaluation. As support for the care provider and executives, SALAR provides a patient safety manual, ”Risk analysis and incident analysis” (”Riskanalys och Händelseanalys” ISBN 978-91-7585-237-9). It includes the following scale for rating ***severity*** and ***consequences*** connected to risk analysis:

4. Catastrophic Death/suicide or permanent, debilitating disability

3. Significant Permanent, moderate disability or an extended care period, or a higher level of care required for three or more patients

2. Moderate Temporary disability or an extended care period, or a higher level of care required for one or two patients

1: Minor Discomfort or minor harm

One of the cornerstones in healthcare regulations is that the benefits of the care given should greatly exceed the risks that the care entails.

IT security

IT security, described in the standard family SS-ISO/IEC 27000, refers to the efforts taken to prevent the dispersion, corruption and destruction of data and to ensure that data are available when necessary. This depends upon three basic requirements:

- **Confidentiality** Do you have the right to partake of the data?
  The care relationship with the patient and, in some cases, patient consent.
  Authorization control.

- **Integrity** Can you rely upon the correctness of the data, that it is not corrupted or an artefact?

- **Availability** Is the data available to an authorized person when needed?
    - The concept of Availability also contains requirements on **Traceability** - Who has had access to the data and when?

IT security relates to:

- Infrastructure for technology and data management.
- Policies for technical security requirements and routines serving to guarantee IT security.
- Measures relating to design of hardware, software, clients, servers, databases, authorization control, segmenting, firewalls, data encryption, data backups, virus protection, patch upgrades, etc.

These measures have in common that they serve to both proactively and reactively protect data and data processing.

Information security

Information should be protected so that it is not intentionally made available or revealed to unauthorized persons or used in a prohibited manner. Information security serves to protect the privacy of the individual. Risk analysis of information security serves to show the level of **consequences** (which is the term within information security corresponding to ”level of severity” in patient safety) for an individual if information is disseminated unlawfully.

The below scale originates from the Swedish Collaborative Group on Information Security (Samverkansgruppen för informationssäkerhet, SAMFI), which consists of a number of authorities, all of which have responsibility for information security in society. Within this field, there is no national consensus between counties/regions equivalent to the patient safety handbook of SALAR. For example, the care provider Region Skåne defines the consequences of loss of confidentiality as follows:

4. **Very serious** Information where loss of confidentiality entails grave/catastrophic negative effects for the organization or another organization and its assets, or for an individual, in particular one with a protected identity.
    - Information covered by specific legislation, e.g., PDL.

3. **Serious** Information where loss of confidentiality entails significant negative effects for the organization or another organization and its assets, or for an individual.
    - Personal data in general or which, under PUL, are to be seen as sensitive.

2. **Minor** Information where loss of confidentiality entails moderate negative effects for the organization or another organization and its assets, or for an individual.

1. **Negligible** Information for which there is no requirement of confidentiality or where loss of confidentiality does not entail any, or only minor, negative effects for the organization or another organization and its assets, or for an individual.

An information safety risk analysis should be performed for all three perspectives: confidentiality, integrity and availability.

The EU Data Protection Reform

The EU *Data Protection Reform* is realized through new legal acts on processing personal data (GDPR). The reform will enter into force in May 2018. According to DI, the General Data Protection Regulation encompasses, among other things:

- More, and more precise, definitions of various terms such as consent, genetic data, biometric data, etc.
- Clearer rights for individuals, such as the right to demand that personal data be erased and the right to gain access to personal data in order to transfer them to another supplier of electronic communication services.
- Clearer rules of liability for those processing personal data, such as personal data controllers and personal data assistants.
- Rules on increased collaboration between the data protection authorities of the EU member states, and a so-called *One-stop-shop mechanism*.

Recommendations on balancing protection of life and health with protection of patient privacy

Guidelines

The general perception among actors operating in the field is that it is important to balance the requirements on measures to protect individual privacy with the requirements on significant protection of life and health. There are, however, no guidelines on how to act in practice to achieve a balance between these interests. The feedback given LfMT thus far, in the dialogue with various Swedish authorities and other actors in the country, is that both interests should be guaranteed in so far as possible.

Given the lack of tangible instructions and guidance, LfMT suggests the following recommendations be used until such time that our authorities present clear information:

A. If there is no conflict between performing measures needed to protect ”Life and health” and measures prescribed to protect ”Patient privacy,” we recommend that these measures are performed in their entirety. However, it is important that measures performed in each area are also subject to risk analyses, in which both aforementioned aspects are taken into account, so that the protective measures in themselves do not entail the introduction of new risks to ”Life and health” and/or ”Patient privacy.”

B. If there is a conflict between performing measures needed to protect ”Life and health” and measures for ”Patient privacy,” the measures should be balanced in accordance with model for balancing risks proposed below.

Model for balancing risks

LfMT recommends that time criteria are used to balance the protection of life and health with patient privacy.

To achieve a balance between protection of ”Patient privacy” and of ”Life and health,” LfMT recommends that the assessment is made with time criteria, a concept originating in Swedish ambulance care. We want to emphasize that these time criteria are not the crucial point. It is the medical assessment of the patient’s status, performed by care personnel, that provides guidance.

The time criteria below, based on the need to access patient data, are to be used as a guideline for the maximum permissible time it takes to remove any obstacles to access of a patient’s personal data:

4. Very large	Time-critical emergency, life-threatening (action within 15 minutes).
3. Large	Emergent, not life-threatening (action within 60 minutes).
2. Small	Urgent, with reasonable lead times (action within 4 hours).
1. Very small	A delay will not affect the patient’s condition (action can be delayed by more than 4 hours).

When a MD contains very important personal data about a patient, to which healthcare staff must have immediate access, the authorization control mechanism should be independent of the MD. See the following reasoning on authorization control. Examples of such MDs are heart monitors at cardiac intensive care units (CICU) and blood gas tests at birth centres.

Confidentiality regarding authorization control

Care provider shall establish regulations and conditions for granting authorization to access such data on patients that are processed entirely or partially automatically. Such authorization shall be limited to what is required in order for an individual to perform his/her tasks within the healthcare system. Care providers must, under PDL, ensure that it is possible to review who has made use of the ability to access such patient data. The legislation makes clear that it is important to ensure both verification and follow-up of the care relationship between a patient and the personnel granted access to the patient’s personal data.

The care provider shall establish regulations and conditions for granting authorization to access *MD data* that are processed entirely or partially automatically.

The aforementioned time criteria can also be used as a general guideline on a suitable level of authorization control, in accordance with the following categorization proposed by LfMT, which is based on the need to access patient data:

4. Very large Time-critical emergency, life-threatening patient condition.

- External authorization control/perimeter security, i.e., no internal authorization control in the MD to verify a person's identity before access is granted to a patient's personal data (e.g., service records).
- Synonymous patient ID (e.g., ”Room 4:2”).

3. Large Emergent, not life-threatening patient condition.

- Internal authorization control in MD with single-factor authentication, plus a requirement on the possibility to bypass authorization control.

2. Small Urgent, but reasonable lead times are acceptable.

- Internal authorization control with two-factor authentication, plus a requirement on the possibility to bypass authorization control.

1. Very small A delay will not affect the patient's condition.

- Internal authorization control with two-factor authentication, without a requirement on the possibility to bypass authorization control.

As an example of authorization control, systems with risks at level 4, ”Very large – Time-critical emergency, life-threatening patient condition,” should not use a technical authorization system for the relevant MD. Patient privacy should be protected through external, manual control or control of which people are given physical access to the area where access to the MD in question is possible, and through ensuring that this area is open only to authorized personnel with patient relationships, with access to the personal data needed for them to perform their tasks.

The technical design of authorization control for MDs should fulfil relevant requirements in MDD. This falls under the manufacturer's responsibility.

The head of operations has extensive responsibilities as regards design and follow-up of authorizations and access control. Individual healthcare workers and those working with technology also have extensive responsibility in self-evaluation of their own authorizations and the data they can access, as well as actively preventing accidental dissemination of patients' personal data.

In the design of authorization systems, one must be aware of the fact that patients in most cases have actively sought medical care and expect the healthcare organization to use pre-existing care-related information about them to their benefit. Everyone should therefore strive to create the conditions to make valuable, historic information available when it is needed at an instance of care.

Integrity and Availability

Balancing IT security to guarantee the integrity and availability of information relates to the development of standardized technological platforms and processes for development and maintenance of an IT environment.

Client, server and communication platforms tailored for MDs should be developed. In parallel, policies for technological security requirements and routines should be established in order to safeguard IT security. MD manufacturers should adopt a more proactive stance. The current development shows that they often shift from using custom software to using standardized IT components from large suppliers, such as Microsoft and Adobe. We know that these IT components are updated continuously. The manufacturers should therefore in their risk analysis pre-approve such updates, rather than review them reactively, as is often the case now, with implementation performed long after potential security flaws have been identified. Quality assurance of these pre-approved updates should be performed through both risk analysis and use of a vigilance system.

The aforementioned time criteria should also serve as guidelines for the fields of integrity and availability. If the intended use of an MD is to manage life-threatening situations in a patient, the above model for balancing risks indicates that it is crucial that security flaws are managed quickly. The consequences for a patient of an e-virus attack can determine whether or not the patient suffers healthcare-related harm. There are suppliers of vital MDs that currently take months to approve urgent updates. This is a highly unsatisfactory state of affairs!

The MD sector, including affected authorities, interest organizations and manufacturers, must work together to change the perspective, so that IT security management shifts from a reactive to a proactive approach.

Recommendations

LfMT's recommendations for managing the four problems areas from Part 1 and above are:

1. **The extent to which design of information security and authorization control negatively impacts upon efficiency in healthcare and thus entails a risk of physical harm to patients either through erroneous diagnosis and treatment or through failure to take medically necessary measures.**

   1.1. Recommendation:
   - Ensure that the design of MD use is based on the use intended by the manufacturer.
   - Ensure that the care provider's use of patients' personal data is based on the criteria proposed in the section *General guidelines/Confidentiality regarding authorization control* above, so that a balance can be achieved between a patient's rightful demands regarding both ”Life and health” and ”Patient privacy.”

2. **The extent to which flaws in the design of information security as regards authorization control contribute to intentional or accidental dissemination of patients' personal data, so that the privacy of patients is harmed.**

   2.1. Recommendation:
   - A patient's personal data, including *MD data,* should in so far as possible be encrypted.
   - *MD data* should be processed inside well-defined and protected logical areas (using firewalls and similar solutions).

3. **The extent to which MD manufacturers are liable to, in their risk management processes, balance and safeguard the protection that each patient can rightfully expect against physical harm and against breaches of privacy.**

   3.1. Recommendation:
   - The Medical Products Agency should give manufacturers clear guidelines to, in their risk analyses, identify and mitigate risks to the protection of both ”Life and health” and ”Patient privacy.”

4. **The extent to which authorities can clarify the regulations on *MD data* on the path from registration of biological parameters in a patient to being entered as test results in a medical chart.**

   4.1. Recommendation:
   - The authorities SoS, IVO and LV should, as per the reasoning above, create and publish instructions on how MD data should be viewed and when such data are to be seen as matters of medical record.
   - The Ministry of Health and Social Affairs and the Ministry of Justice should, in connection with the EU's ongoing amendments to MDD and GDPR, strive to harmonize the sections regulating information processing within healthcare and with MD in PSL, PUL, PDL and LMP.

Specific requirements on manufacturers and care providers

The manufacturer:

- Is charged with fulfilling stringent requirements on the protection of life and health through medical devices. This includes information security.
- Shall clearly state if a certain MD is intended for use in keeping or processing medical chart data or is to be integrated with another MD or system intended for keeping chart data (e.g., through integration).
- Shall report to the Medical Products Agency any significant problems and issues related to authorization systems and information security in their products.

The care provider:

- Does not have the main responsibility for design, construction or implementation of integrity protection in MDs from external manufacturers, when MDs are used for their intended use.
- Shall report flaws in authorization systems and information security to both the Medical Products Agency and the manufacturer of the MD in question.

Both the manufacturer and the care provider:

- Must improve the balance in MDs between privacy protection and protection against physical harm to patients.
- Must ensure that the design of information access is appropriate for the product's intended medical use.

Proposed future tasks for LfMT

- To pursue the following matters, in dialogue with affected Swedish authorities and ministries, such as the Medical Products Agency, the National Board of Health and Welfare, the Health and Social Care Inspectorate, the Swedish eHealth Agency and the Swedish Data Protection Authority:
  - In connection with the transformation of MDD into an EU regulation, MDR, supplement the regulations with instructions to both manufacturers and care providers on how information security in MDs should be designed and managed.
  - Revise PDL, so that it harmonizes with both the new EU regulation, MDR, and PSL.

- End of document -