PHILIPS

Interoperability Solutions

White paper

Privacy protection and sharing medical information

Index

Privacy protection and sharing medical information; is this a contradiction in terms?

Various media discuss the importance of protecting privacy-sensitive medical data with great regularity. In Europe even more so since the General Data Protection Regulation (GDPR) came into force in 2016. The healthcare sector is, amongst others, worried due to the obligation to report whenever a serious leak has been detected, and because the penalty has increased exponentially.

Traditionally, a doctor managed the files of his patients. These files mainly consisted of hard copy folders that were stored in some cabinet close to the doctor. As such, access to these files used to be limited to those persons that could physically reach them. Nowadays, doctors increasingly use a central information system which logs medical information in digital files. This is highly convenient. Just press the button and the medical files scroll across your screen. However, it does have a downside, as medical files are now accessible to more staff members than may be necessary.

A new dimension was added over the past few years. Focus on cost savings in healthcare has led to more intensive types of collaboration between healthcare providers. Hospitals tend to specialize. Various healthcare institutions are merging to allow for better coverage of healthcare services in a region. Healthcare insurers are cautiously attempting to control healthcare provision so that we, the patients, cannot always turn to our familiar hospital.

As a consequence of these developments our medical files have been fragmented across various healthcare providers, institutions, and information systems. When we have to visit various sites to get healthcare services, it is highly convenient if our doctor can obtain our medical data that have not been recorded in his own systems.

Obviously, you think: no problem. This problem has been tackled in other sectors a long time ago. It only requires a link-up of systems through the internet, and we'll be up and running. Similar issues have been solved a long time ago in the financial sector, for instance. As a consequence, we can securely transfer money between current accounts held at various banks.

Unfortunately, it is not that simple. That is because this concerns medical information which is privacy-sensitive. Who will determine who can request what information? Who will guarantee that information will be shared securely? And, what will happen to our information?

In short, these are conflicting interests.

Protecting personal health information

Every day, we are faced with these conflicting interests as Philips Interoperability Solutions provides solutions that enable sharing of healthcare information between healthcare providers. In order to clarify the conflicting interests even further, we will add yet another dimension. This is the dimension that the doctor, who needs access to our medical information, requires access from another site, and by means of another information system, than the site and the information system that have recorded said medical information. In other words, the systems that has the records with medical information must decide whether it will allow access to the information to a user that is unknown to the relevant system. This is a dilemma.

It splits up the issue of access to medical information into a number of queries:

1 **Who is this person who wants to inspect my medical information?** (identification, authentication)
2 **Is this person authorized to do so?** (authorization, legal framework)
3 **In case medical information is shared, will it be done in a secure manner?** (data transport security, encryption)
4 **What is my say in the matter, as a patient, about who can and cannot access my medical information?** (consent)

Who wants access to my information?

The first query pertains to authentication. Before we can decide on access to medical information in the first place, we want to know the identity of the person that requests access. Authentication in information systems is executed by unambiguous assessment of the electronic identity of the user that has logged on.

Philips Interoperability Solutions supports a number of authentication options to this end:

1. Based on a **user profile** that is recorded in an external system (LDAP)
2. Based on a **smart card** on which the user profile is recorded
3. By the **operating system** that operates the Philips Interoperability Solutions application (Integrated Windows Authentication)
4. Based on an **SAML token** that is forwarded by an external application (SSO)

Philips Interoperability Platform uses a number of IHE profiles which are relevant to this end:

- **Enterprise User Authentication** – This profile records how to share information with an external authentication system (e.g. Windows Active Directory) based on Kerberos standard authentication
- **Cross-Enterprise User Assertion** – This profile records how user authentication information can be shared between two systems.
- **Healthcare Provider Directory** – This profile records interaction with a healthcare provider directory so that a system can find out at what organization/department a user is employed. Moreover, this profile provides the option to record a number of user characteristics. These may include contact details, email addresses, and so on.

These profiles record how authentication information can be shared. The second query will clarify how this authentication information is used to determine what a user will be authorized to do.

Who is allowed access to my information?

Query two pertains to authorization. This is a more complicated topic since authorization can only be demanded by an information system. Authorization itself is a matter of agreement or policy. E.g. the agreement that doctors will only have access to medical files of patients that they attend to. If there is no clinical relationship, access to files should be denied. Philips Interoperability Solutions offers software products that allow you to define authorization rules. This is based on the XACML standard. A and C represent “Access Control” that is recorded in XML rules.

The XACML standard provides a lot of choices. Philips Interoperability Solutions limits these choices to a number of practical options that allow for defining authorization rules for both persons and systems. One example of an authorization rule for persons is: “each user with the registered role of doctor can inspect medical documents of the hospital that employs him/her; inspection of any other documents requires authorization from the patient”. One example of an authorization rule for systems is: “system A is allowed to link up with system B”.

Unfortunately, it is sober reality that a lot less is standardized in the field of “access control” than we would like. Many information systems solve this in their own manner. Consequently, Philips Interoperability Solutions offers the opportunity to enforce an “access control” policy centrally, by means of the XDS Registry. This will allow for recording in one location who can inspect what information. Additionally, Philips Interoperability Solutions provides comprehensive “audit logging” options, so it can be assessed at all times who had access to patient data from what system and at what time.

Will my data be shared securely?

Question three pertains to secure electronic sharing of information between systems. A number of standard techniques, such as “Transport Layer Security (TLS)” are available to this end. This is commonly known as Secure Socket Layer (SSL) encryption on the internet. And it is often also described as a “private VPN tunnel”. IHE also provides a solution in this respect, by means of the ATNA profile.

Philips Interoperability Solutions demands mutual system authentication based on this profile. This means that two systems that share information must trust each other based on security certificates that have been agreed on in advance. Encrypted information can only be shared when both systems accept each other’s certificate.

How can I monitor who has access to my information?

The fourth and final query pertains to approval by the patient. This is also known as “patient consent”. Whether it is pursuant to a legal guideline, a Code of Conduct, an advice by a national data protection authority, or a guideline of a patient association, patient consent is always based on the fact that it can be recorded and used to assess who can be authorized to inspect the medical file. Here as well, Philips Interoperability Solutions provides a solution based on the IHE profile. The Basic Patient Privacy Consent (BPPC) facilitates electronic recording of the consent requested from the patient.

However, Philips Interoperability Solutions takes it to the next level. The “consent document” can be used in the above-mentioned authorization rules so that the patient’s consent can be taken into account when deciding whether a doctor will or will not have access to the file.

Recording consent by means of Philips Interoperability Solutions products can be effected both manually and automatically. In doing so, it is important to be aware that a protocol must be introduced by which a patient is asked to give consent, prior to being able to record consent.

One option is that a patient will be informed about the hospital’s privacy policy during the intake at the registration desk of a hospital. The request for consent can be submitted and recorded during a consultation with the doctor. Every healthcare institution will have to introduce its own policy in this respect.

Obviously, we will also consider trauma situations when access to the file is required and the patient will be unable to give consent. In that case, Philips Interoperability Solutions offers a “break the glass” option in which a doctor can authorize himself to inspect a file. However, any access to this file will be logged and audited in a special manner.

Finally, the three-tier model

This whitepaper has addressed but a few of the aspects that are relevant to the protection of privacy-sensitive (medical) patient data. Protection of this data entails measures that limit access to this information to those persons that have been authorized accordingly.

The options to protect medical data effectively that are unique to Philips Interoperability Solutions can be summarized in a three-tier model:

- **Transport tier:**
  System certificates (PKI) and data encryption
- **Application tier:**
  Authentication, authorization, audit logging
- **Information tier:**
  Consent management (opt-in, opt-out), role-based access control

All functionalities provided by Philips Interoperability Solutions are based on interoperability profiles that have been drawn up by the international IHE organisation. These profiles offer you, as a user, the best possible guarantee to a vendor-neutral and future-proof solution.

4522 991 60161 * MAY 2020

www.philips.com/interoperability-solutions