IHE EUROPE
Integrating the Healthcare Enterprise

IHE perspective on the European Union GDPR

This whitepaper shows how IHE helps understand the General Data Protection Regulations - GDPR - the influence it has on the use of IHE Profiles and the actions that need to be undertaken as a priority to comply and stay compliant

The EU General Data Protection Regulation and how IHE can help

Effective 14 April 2016 the EU Parliament has approved the General Data Protection Regulation (GDPR[1]) replacing the Data Protection Directive 95/46/EC. On 25 May 2018 the transitional period ends and the GDPR takes effect. Unlike a directive, a regulation does not require national governments to pass any enabling legislation; a regulation is directly binding and applicable[2].

The GDPR uses the 1953 "Convention for the Protection of Human Rights and Fundamental Freedoms" as the' basis for the protection of individual-related data. Over time data protection in the EU has become more enforceable. These are the reasons one should look closely at the GDPR.

What is new in the GDPR?

"This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of their personal data" (Art. 1(2) GDPR).

In general, data as defined by the GDPR may not be processed unless the conditions that allow the processing[3] of personal data as described by the GDPR are met.

The GDPR defines processing as any operation, or set of operations, which is performed on personal data[4], or on sets of personal data, relating to a natural person (collection, storage, adoption/alteration and retrieval - anything you can do). It does not apply to data concerning legal persons (e.g. companies).

The EU has substantially expanded the definition of personal data under the revised GDPR that takes effect in May 2018. The principles are extended to any information concerning an identified or identifiable natural person, including pseudonymised[5] data.

Only data that can't be retraced to the individual person by any means can be processed without being inconsistent with GDPR requirements.

Personal Data can only be processed if there is a legal provision.

The GDPR defines a set of legal bases for processing. The primary basis for processing data in healthcare (as special category data) would be a legitimate relationship under Article 9(2). In the case of a seriously ill patient the vital interests' clause could be applied (especially as described under "Accident and Emergency"). In many cases, however, consent may be invoked as a requirement.

When health related data is processed based on consent[6], is not only freely given, specific, and unambiguous, but also that it is explicit. This means that when health data (or other sensitive data) is processed it is imperative that full information about the nature of the data collected and the use of it is provided to the data subject and that consent for

1 EUR-LEX – access to European Union law: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), online http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX%3A32016R0679.

2 Although the GDPR text provides derogations (opening clauses) allowing the Member States to adopt variations and additional requirements on a given topic.

3 Art. 4(2) GDPR: 'processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

4 Art. 4(1) GDPR: 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

5 Art. 4(5) GDPR: 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data is not attributed to an identified or identifiable natural person.

6 Art. 4(11) GDPR: 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

those specific purposes is explicitly provided. While the law does not state that such consent must be written, requiring a data subject to sign a statement of consent may often be the simplest way to demonstrate compliance for sensitive data. Controllers[7] must ensure personal data is processed lawfully, transparently and for a specific purpose.

What does the GDPR regulate?

The GDPR requires that controllers[7] and processors[8] must be transparent about how they collect data, what they do with it, how they process it and with whom it will be shared. Controllers must also be clear in explaining these things to the individuals whose data is being processed. Among other issues, the GDPR describes principles as well as it defines requirements for:

— the conditions when access to personal information is allowed;
— ensuring fair and transparent processing regarding the access to personal data and taking into account conditions and context by profiling and implementing technical and organisational measures;
— actions when an illegal access to personal data has been discovered (e.g. reporting of a data breach);
— individuals whose data is being processed, especially the rights:
  - to gain access to their personal data (including data portability) and to exercise that right easily and at reasonable intervals;
  - to rectify and erase their personal data (within the existing legal constraints).
— actions to guarantee the privacy and security of such treatment, especially:
  - adoption of “internal policies and implement measures that meet the principles of data protection by design and data protection by default”;
  - the implementation of technical and organisational measures to ensure a level of security;
  - appropriate to the risk for the rights and freedoms of the persons whose data is being processed;
  - how to carry out a privacy impact assessment if necessary.
— the engagement for data protection officers;
— the penalties in case of non-compliance.

Furthermore, the GDPR demands that the controller is responsible for complying with the GDPR.

Who is affected by the GDPR?

It affects **everyone** who

— processes personal data in the context of an undertaking established in the EU, regardless of where the processing takes place;
— or provides services involving the processing of individual-related data of anyone in the EU, regardless of where the undertaking is established, or the nationality of the individual.

Due to the nature of the data upon which the healthcare system works the GDPR should be of particular interest to anyone in the health care business (vendors, healthcare professionals and anyone involved in the processing of patient data alike).

7 Art. 4(7) GDPR: ‘controller’ means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination, may be provided for by Union or Member State law.

8 Art. 4(8) GDPR: ‘processor’ means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Why should anyone care more about the GDPR than its predecessors?

For the first time there are significant fines connected to non-compliant behavior. Up to 20 Million Euro or 4% of the total worldwide annual turnover of the infringing organisation or institution in the preceding financial year – whichever sum is higher.

How is interoperability in health based on IHE Profiles affected by the GDPR?

In general, any implementation of an IHE Profile that defines the exchange or processing of personal data is affected. The GDPR requires that "the processing of personal data" (which clearly includes the sending and receiving of patient data) is done on one of the allowed legal grounds defined by the GDPR.
Besides the legal grounds for processing, the GDPR, for each processing, "… requires the appropriate technical and organisational measures to ensure a level of security appropriate to the risk …". It also defines that these measures "… meet in particular the principles of data protection by design and data protection by default." Some IHE Profiles may include technical measures that contribute to meeting one of more of the GDPR requirements.
Any project deploying IT systems and devices that implement IHE Profiles has to fulfill the requirements of the GDPR: they have to meet the technical requirements (like data protection by design/ default or the possibility to fulfill the rights of the individual (e.g. confidentiality, privacy, availability).

For example, ask yourself the following questions of 'your' use or design of an IHE Profile:

— Is each interface implemented (to each single party) supported by a legal ground for collecting and exchanging data? (Art. 6 GDPR)
— When data processing is justified by patient consent, are appropriate measures for documenting the declaration of consent obtained from the data subject? (Art. 7 GDPR) (Art. 7 GDPR)
— Are appropriate measures to support the withdrawal of consent in place? (Art. 7 GDPR)
— Is there a process to check that transparency requirements are met before processing starts? (Art. 12 GDPR)
— Is there any possibility for providing information to the data subject to make the entire data processing process transparent? (Art. 13,14 GDPR)
— Can a request from the data subject to obtain access to their personal data (metadata included) within the requirements of GDPR, and other legal constraints, be met? (Art. 15 GDPR)
— Can a request for erasing all personal data (metadata included) of a data subject be met? (Art. 17 GDPR)
— Can the right of restriction of processing be met? (Art. 18 GDPR)
— Can a request to receive the personal data in a structured, commonly used and machine-readable format and to transmit it to another controller be met? (Art. 20 GDPR)
— Is all information declared as 'mandatory' in an IHE Profile really necessary or required for the purpose that is supposed to be performed? (Art. 25 GDPR)

If any of the above questions is answered negatively the deployment, or implementation of the IHE Profile in question, needs to be reviewed in order to be used in a GDPR compliant manner. This list is not exhaustive. It represents only examples of the issues that need to be dealt with.

In the second part we will focus on the impact on GDPR on interoperability and how IHE can help deploy interoperable systems that are GDPR compliant.

How does GDPR influence the use of IHE Profiles?

It influences the implementation of any process or system that manages personal information. The person responsible needs to be sure that the requirements of the GDPR are met. This may require different types of measures:

- the IHE Profiles have to be enhanced (e.g. by combining it with another Profile that addresses the identified gap);
- the IHE Profiles need to be supplemented in its specification by IHE itself;
- the system implementing the IHE Profile needs to be redesigned;
- the organisation managing the deployment of interoperable systems need to set the correct policy.

As shown above, interoperability is only one of the areas that need to be addressed to achieve GDPR compliance.

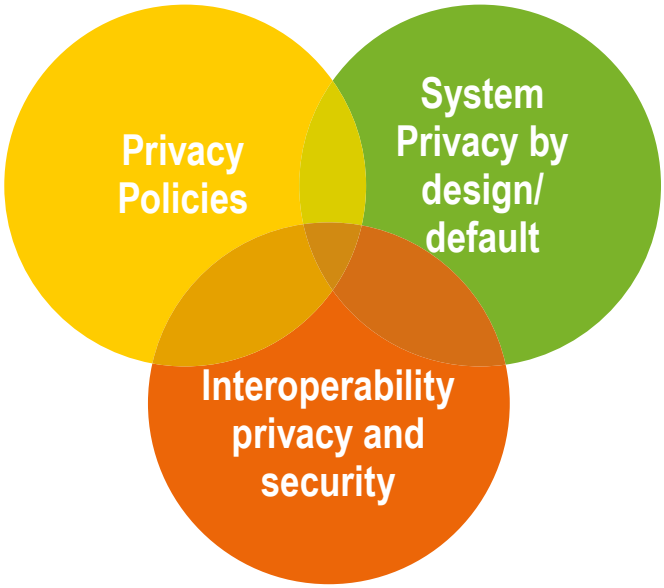

Fig. 1 - High level topics addressed by GDPR

Although there is much to do in setting the necessary policies and ensuring that the systems that are deployed are designed with privacy in mind, IHE would like to ensure that it makes GDPR compliance easier when IHE Profiles are used.

This document will mainly focus on the “orange” area, including its intersection with the “yellow” and “green” areas of Fig. 1 - High level topics addressed by GDPR.

Can IHE help in facilitating the adoption of GDPR?

It is a very demanding task to deploy interconnected systems exchanging personal data in a GDPR conformant environment. Due to the great variety of workflows and IT systems involved this is a task that could be simplified by using combined forces of a larger community – such as IHE. We believe that this simplification could be a further benefit of adopting IHE Profiles.

GPDR defines specific policy requirements for data access and portability which can be addressed in part by interoperability. This is the core competence of IHE and a topic with which IHE has much experience, in particular in the area of regional and national health information exchange with the family of the XD* Profiles (XDS, XDS-I, XDM, MHD…). Some topics of the GDPR have been already addressed by IHE Profiles e.g. Profiles on patient consent (BPPC and APPC), access logging (ATNA). However, they must be evaluated to see if they fully comply with the applicable GDPR requirements.

Interoperability and GDPR

GDPR encourages interoperability (Article 20 – "Right to data portability"): "The data subject shall have the right to receive the personal data …., in a structured, commonly used and machine-readable format …" In addition, the conditions referred to in recital 68 above are relevant: "[...] the data subject should also be allowed to receive personal data […] in a structured, commonly used, machine-readable and interoperable format […]. Data controllers should be encouraged to develop interoperable formats that enable data portability."

But it comes with a cost. The use of personal data in a deployed set of interconnected systems to achieve a use case/ process must fulfill the relevant GDPR requirements. This means for IHE that each Profile must be reviewed to determine which specific GDPR requirements need to be addressed, and then possibly revised for each intended/ stated use case. The three following examples will illustrate this:

1. Push of patient identified health information from one health professional to another using email;
2. Push of patient health information from one health professional to another using media interchange;
3. Pull of patient identified health information from an electronic health database.

(1) Push of patient identified health information from one health professional to another using email

In this scenario, physician A sends patient related health information to physician B via email using the XDM Profile.

- The XDM Profile does not address how physician A gets access to the data nor does it check the patient consent or another legal group of processing(Art 9 (2)(a)) (Art. 9 (2)(c) – vital interests; or 9(2)(h) - healthcare; or 9(2)(i) – public health; or 9(2)(j) – research)) for this transmission. These topics are addressed either by other Profiles or simply by the application gaining access to the data.
- The processing of the email must take place on a system where access is solely limited to authorised users and the access is logged (Art. 5(1f), 32 (1b) GDPR). XDM defines the grouping with ATNA, which in principle addresses the requirements of the GDPR. But the ATNA Profile needs to be evaluated to ensure it meets all the requirements for an access log for this specific use case.
- As being responsible for the data, physician A must ensure that he sends the data only to the health professional physician B which the patient has consented to, or which he can justify sending based on one of the other legal bases for processing health related data. In the case of XDM using email, two measures are needed. First, the payload should be encrypted using an end-to-end encryption with valid and authenticated X.509 certificates (Art. 32 (1a) GDPR). That way physician A can be certain that only physician B can decrypt the information. Second, in order to retrieve the email from the email server, physician B must by authenticated by the mail server (e.g. using a username and password). This also addresses the GDPR requirement for confidentiality within the transfer of personal data (Art. 5(1)(f), 32 (1)(b) GDPR).
- The security requirement for integrity of Art. 5(1)(f), 32 (1)(b) GDPR can be solved by using an electronic signature with the same certificate as used for the encryption. Both are defined by the XDM Profile.
- Physician A must be certain that physician B actually receives the email. This topic is addressed by the XDM
- Profile defining the use of the MIME notification mechanism.
- The GPDR requires that access to personal data is logged, and that all access to data can be demonstrated reliably in the case of a dispute. XDM groups the actors with the ATNA Profile. From an IHE perspective this meets the requirements for the XDM Profile, but it is still necessary to analyse if the ATNA Profile meets all the GDPR requirements regarding the content of such a log.

(2) Push of patient health information from one health professional to another using interchange media

In this scenario, physician A sends patient health information to physician B via CD-ROM by handing it to the patient, using the XDM Profile.

- The XDM Profile does not address how physician A gets access to the data nor does it check the patient consent

or another legal ground for processing (Art. 9 (2)) for this transmission. These topics are addressed either by other Profiles or simply by the application gaining access to the data. Consequently, using the XDM Profile does not guarantee compliance with these two GDPR requirements (restricting access to personal data, retrieving permission to sending data)

- The processing of the CD-ROM must take place on a system where access is solely limited to authorised users and their access is logged (Art. 5(1)(f), 32 (1)(b) GDPR). Like in use case 1, XDM defines the grouping with ATNA, which in principle meets the requirements of the GDPR. But the ATNA Profile needs to be evaluated to establish if it meets all requirements for an access log for this specific use case.
- The CD-ROM is handed out to the patient. Physician A must be sure to hand over the right media to the right patient. This procedure must be documented in a GDPR data compliant log system, but is out of scope for the XDM Profile. As the media is handed over to the patient, the patient is now responsible for the secure transport and confidentiality of the data.
- If the media had been given to another person or sent by post the media would need to be encrypted to prevent unauthorised access unless the controller could come up with a plausible explanation for leaving the data unencrypted (Art. 32 (1)(a) GDPR). In any case XDM would have, for this specific use case, to add a mechanism allowing the encryption of the entire personal data on a media, to meet the requirements of the GDPR.

(3) Pull of patient identified health information from an electronic health database

In this scenario physician B retrieves patient identified health information from a medical database which has been placed there by physician A using the XDS Profile.

- The XDS Profile does not address how physician A checks for patient consent or another legal ground for processing (Art. 9 (2)), but allows the sharing of the patient health data in the XDS affinity domain. These topics are addressed by other Profiles (e.g. ATNA, BPPC, APPC).
- To gain access to the XDS domain the user (physician B) must authenticate himself (Art. 5(1)(f), 32 (1)(b) GDPR). Therefore, XDS requires a grouping with another Profile (XUA) which handles this topic. This means that these Profiles must be analysed form a GDPR prospective ensuring that all applicable requirements are met.
- The next step requires checking if the physician B has the right to access patient personal data (Art. 5(1)(f), 32 (1)(b) GDPR). To address this requirement XDS references other IHE Profiles like BPPC and APPC. However these Profiles still need to be evaluated for this specific use case from a GDPR perspective.
- All access to the patient identifying health information by physician B must be logged. Physician A is considered the “controller” and is responsible for the data that is pulled by physician B. Therefore the process needs to be reviewed to see if physician A must be informed about the access to this data (Art. 5) or if logging handled be the ATNA Profile, fulfills the GDPR requirements for this specific scenario.
- All actors holding personal data must ensure that the data is kept in the most secure and safe way available, using state-of-the-art technology, but still facilitating its use. Logging is required for access and alteration.
- Deletion, restriction and portability must be possible as well.
- All communication must be secured to protect the personal data from unauthorised access and alteration, as well as from loss of information. This must be transparent for the users of the data (e.g. ATNA channel encryption).
- How physician B handles the processing and storage of the data is addressed by the GDPR but is not in the scope of the XDS or other IHE Profiles.
- The information above has also been discussed in the white paper on Health Information Exchange: Enabling Document Sharing Using IHE Profiles which will be updated to explicitly address the interoperability impact of GDPR and more recent IHE privacy related Profiles such as APPC.

Conclusion

The examples discussed above highlight the complexity of applying the GDPR to processes in health care and how the requirements are interwoven with IHE Profiles. The good news is that even today IHE Profiles provide solutions by combining security and privacy specific IHE Profiles such as ATNA, IUA, XUA, BPPC and APPC with the Profiles focused on information exchange in cross-border, national or regional ehealth deployments.

In conclusion the GDPR can be an effective catalyst to significantly extend the reach and use of IHE Profiles. Some Profiles or combinations of Profiles already meet GDPR's security and privacy requirements. Others enable the portability of health information which will become a topic for any vendor providing solutions.

The users of IHE Profiles can be assured that the IHE community will work on evaluating and enhancing the Profiles to meet the GDPR requirements.

IHE-Europe aisbl
Diamant Building Boulevard Reyers 80 1030 Brussels, Belgium
E-mail
Follow IHE-Europe on Linkedin
Follow IHE-Europe on Twitter
Subscribe to the IHE-Europe News Pulse

The IHE logo is registered trademarks of IHE-Europe