FHIR - GDPR

Introduction:

The **General Data Protection Regulation** (**GDPR**) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). It was adopted on 27 April 2016 and became enforceable on 25 May 2018, after a two-year transition period. Unlike a directive, it does not require national governments to pass any enabling legislation and so it is directly binding and applicable.

This article is to address the abilities and requirements of the ***General Data Protection Regulation*** *in an environment using a Fast Health Interoperability Resources (FHIR)-based healthcare interoperability. The authors of this paper assume that an understanding of the articles and legal requirements of the G DPR is in place and only address the technical requirements for handling the various requests originating from EU citizens and others within the GDPR affecting regions.*

The Articles of the GDPR affecting healthcare data interoperability are mapped to specific resources and operations showing the possible methods to handle specific Requests and requirements. While not all Requests can be managed purely with technical responses, this paper will highlight FHIR resources and operations that may best be used. [explain not all Articles will be listed if not relevant to FHIR]

In addition, this article will review technical gaps that may need addressing and allow for discussion and feedback on how to potentially eliminated the gaps for a complete interoperability technical solution.

The HL7 members and workgroups have consulted with experts in GDPR and FHIR to create this article and have ensured this represents the latest views and technical understanding. We invite dialogue and comment regarding the content and suggestions herein.

Scope:

This scope of this document is to address the abilities and requirements of the GDPR in an environment using FHIR-based healthcare interoperability.

The scope of this paper is limited to the specific FHIR resources and operations that may best respond to a GDPR request such as a Request for Disclosure or Request for Erasure.

Policy-based decisions will not be addressed and will be left to the organization and legal groups to review and specify. Specifically, policy indications for use-cases, types of data collected, and types of processing are out of scope.

Executive Summary:

This page to be a collaborative effort to map GDPR requirements/needs to FHIR included capabilities (e.g. security labels, provenance, auditEvent, consent, etc); and residual Security Considerations to be addressed by system design, and organization deployment.

GDPR Basics - more than technology

The Privacy Principles that are generally included in many standards and guidance are inclusive of giving the Individual the right of Access, the right of Correction, and the right to control how their data are used. Too often people think Privacy is only about restricting access. The HL7, IHE, and DICOM workgroups have always used the more expansive definition of Privacy Principles.

It is a fundamental truth that GDPR is more than technology. GDPR will drive far more work in the space of writing Policies, Procedures, Communications, and such. There are many publications, consultants, and lawyers that can help with this. There are many publications that explain GDPR to you. The law itself is not that hard to read.

Here are some basic princples about GDPR:

- Processing personal data or sensitive personal data is prohibited unless for very specific reasons defined in article 6 and article 9
- Processing shall only be collected for specified, explicit and legitimate purposes (article 5(1)) and according to article 30 each controller and processor shall maintain a record of processing activities providing information about the data processing (for instance purpose of processing and a description of the categories of data subjects and of the categories of personal data)
- Data minimization
- Privacy by Design: GDPR is very much patterned after "Privacy by Design", indeed it requires that "Privacy by Design" is used.
- Privacy impact analysis
- Data protection officer

GDPR and FHIR - which parts are useful?

The following are the capabilities that are already in the FHIR Specification today and might be useful for GDPR implementation. More details on how they can be used are in the chapters below.

- General principles in the guidances Security & Privacy and Security
- Provenance, Resource
    - Includes a signature mechanism that can be leveraged in many comprehensive ways.

- AuditEvent Resource, and Guidance
- Consent, Resource
- Contract Resource
- *Contract, Resource Kathleen to write a paper about the difference to Consent we can refer to*
- any Resource can be tagged with Security/Privacy tags
- De-Identification guidance
- Secure Communications
    - Common recommended use of TLS (HTTPS)
    - May use Client Authentication
    - Recommend follow good TLS principles such as BCP195
- Authentication and Authorization
    - SMART-on-FHIR - leverage OpenId Connect for User Authentication. Provides a pattern for OAuth scopes
    - IHE - Internet User Authorization - defines a set of OAuth token attributes
    - HEART -- a mechanism for externalized Consent to be managed and Authorization decisions made
- Identity -- various FHIR resources are tied to identities that can be used in Policy (e.g. Consent), and would be used in AuditEvent and Provenance to record Who did some action.
    - Patient
    - RelatedPerson
    - Practitioner
    - PractitionerRole
    - Group
    - Organization
    - Location

“De-identification” of patient’s data can be a strong tool to support the implementation of GDPR, whereas “anonymization” means “removing personally identifiable information (PII) from data sets, so that the people whom the data describe remain anonymous”, and “pseudonymization” refers to any kind of encryption of PII, where the original information can be restored under certain conditions. Anonymized data is no longer person related and therefore not bound to GDPR requirements.

Main principles to be supported by any implementation and their FHIR components

Right for processing personal data / explicit consent:

Requirements

The GDPR distinguishes between personal data and special categories of personal data (sensitive data , e.g. healthcare data)

Where there is no regulatory requirement for data processing you need to get explicit consent from a patient (article 6 and article 9 define the “lawfulness” of processing).

GDPR defines “consent” of the data subject as any freely given, specific, informed and unambiguous indication of the data subject's wishes (article 4(10)). Any policy text presented to get consent must be in an easily accessible form, using clear and plain language and clearly distinguishable from other matters ((article 7(2)). A consent can be withdrawn at any time (article 7(3)).

Impact

It must be clear at any time of collection or processing of personal data on which basis this has been done and for what purpose.

Furthermore whenever processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data (what the patient consented, for what purpose, for what kind of data, for what period of time, has the consent be withdrawn) (article 7(1)).

Legal considerations

Recipient of information is responsible for only processing information for which it has the rights.

FHIR artifacts and its possible usage

Consent resource might be used to hold specific consent on file or to send information about given consent along with healthcare information. To show that querying organization has a valid consent from a patient for a specific class of data and a specific purpose of processing. A list of examples for consent usage can be found here.

Explicit consent always requires a specific purpose of use or purpose of processing. HL7 provides a specific vocabulary to be used in this context. However, it is up to the implementing organizations to negotiate and agree on a specific codeset for interoperability purposes. Specific usage of consent might be specified in an implementation guide (IG). For instance, HL7 works on an IG for use-cases based on HL7 International Patient Summary (IPS).

Use of **contract resource** might be considered in order to accomodate elements that are not in consent (e.g. payment terms, goods and services).

Information about the purpose of processing can be either implicit (e.g. all processed data in a system follows the same principle) or explicitly stored using s ecurity labeling. In the latter the PoU of any consent can be matched against an object's PoU security label to enforce access rights.

Transparency about processing personal data

Requirements

The data subject has considerable rights to get information about the processing of his/her data. This ranges from data a controller has to provide when personal data are obtained to data that has to be provided on request of the data subject. While article 13 and article 14 are about providing general meta-information about the processing to the data subject, article 15 (Right to access) requires providing details. Information shall be provided in writing, or by other means, including, where appropriate, by electronic means (which actually can also be a PDF document).

Impact

The right for transparency requires providing a lot of information about processing of personal data within a limited timeframe. This means a controller needs to keep track of the processing of personal data and provide information for instance (but not limited to)

• What category of personal data is processed for what purpose?

• Where did it come from, based on which consent and for what purpose?

• Are the personal data intended to any other party (especially to a non-European country)?

• Where did it actually go to? *(Third party?)*

Legal considerations

Transparency must not impact the privacy of other people related to a specific person's data (*$TBA: discussion around: does a practisioner give up his/her privacy rights. Pseudonymization?*). Any person requesting information about processed data must be clearly identified.

FHIR artifacts and its possible usage

To store information about data sources either AuditEvent or Provenance can be used.

Provenance is a record that describes entities and processes involved in producing, updating, delivering, or otherwise influencing resources. Provenance provides critical foundation for assessing authenticity, trustability, and traceability. Who authored and why, who updated and why, where were these changes, when were these changes, and what influenced these changes. Audit is used to capture all actions upon data, but also actions upon other protected resources. The Audit log exists to provide evidence that a system is working properly, and thus is used to detect when it is not working properly. So it is used to detect failures in Confidentiality, Integrity, and Availability (see https://healthcaresecprivacy.blogspot.com/2016/03/provenance-vs-audit-it-is-not.html).

Thus, one can use AuditEvent to keep track where data has been sent to, but can use either AuditEvent or Provenance to track where data originally comes from (who authored it). Provenance has to be used when data received from a third party gets modified and redisclosed.

If a system uses different purposes of use to process data, Security Labels can be used to tag data.

To catorize data, the confidentiality classification vocabulary as well as the sensitivity classification vocabulary can be used.

Right to rectification and right to erase (“right to be forgotten”)

Requirements

Article 16 defines the right of the data subject to obtain the rectification of inaccurate personal data with undue delay. Article 17 enables the data subject to request the erasure of personal data concerning him or her without undue delay (specific limitations apply! Especially data must not be erased when there is another legal requirement, e.g. for archiving medical documentation).

Furthermore article 19 requires the controller to communicate any rectification or erasure of personal data or restriction of processing carried out in accordance with Article 16, Article 17(1) and Article 18 (“right to restriction of processing”) to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort.

However, at the end of the medical records retention period information has to be erased or at least anonymized.

Impact

Especially the requirements of article 19 require to track all systems and persons where personal data has been disclosed to.

Legal considerations

Erasure includes ALL data stored and processed for a specific person (even AuditLogs holding references to a patient's data). Any person requesting information about processed data must be clearly identified.

As the processing of healthcare data is often based on specific legal requirements, it can not be clearly said what data has to be purged and what must not be deleted. Therefore it is strongly recomeded to get in contact with your layer!

FHIR artifacts and its possible usage

AuditEvent can be used to keep track where information was sent to.

Possible gaps

A “delete” operation that provides support to delete all data for a specific patient.

Right for portability

Requirements

Article 20 (“Right for portability”) allows the data subject to ask for his or her personal data in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller.

Impact

Effectively this means a controller has to provide all stored personal information about a patient in an interoperable format either exported or directly to a third party.

Legal considerations

This is only relevant if the processing is based on an explicit consent (which means it is unneeded in case processing is based on legal requirements and there is no explicit consent).

In light of Article 20, Paragraph 4, specific consideration needs to be given to information linked to multiple patients. Where data may have been linked (e.g., patient information linked to others with familial or social determinant link or via data analysis) some thought needs to be given on how and what information that may identify a third party will be filtered and/or de-identified and/or omitted in order to preserve the privacy and other GDPR rights of that third party. For example, FamilyMemberHistory may contain information that, if transmitted intact, may violate the right to privacy and require explicit consent.

FHIR artifacts and its possible usage

All FHIR resources used to provide healthcare information regarding any orders, observations, care plans or other healthcare-specific information. This may include all information including resources having financial information (e.g., Contract, Coverage, Claim), or supplementary patient information.

An export or transmission of all patient-linked resources in an acceptable and interoperable format (e.g., application/json or application/xml) to allow ingestion by third party applications is required.

It has to be discussed how information is handled that cannot be currently expressed as FHIR resources. In addition, clarity on information stored on servers linked to the FHIR server and/or of sufficient size (e.g., DICOM information) that would cause difficulty for the sender or recipient is needed.

The operation $everthing on patient can be used to provide all data for a specific patient (which provides a bundle of resources).

General security

Requirements

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate

Impact

Need to implement technical and organizational measures (TOM) to protect personal data.

FHIR artifacts and its possible usage

For detailed information about security refer to http://build.fhir.org/secpriv-module.html and http://build.fhir.org/security.html

	Art		Short	Description	HL7 Component	Usage How to use
Right for processing personal data / Explicit consent: Where there is no regulatory requirement for data processing you	4	(10)	Definition “consent”	‘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	Resource: Co	Use the consent resource to hold specific consent on file

need to get explicit consent from a patient. Information needed: • What the patient consented • For what purpose • For what time • Did he/she retract					nsent	send information about given consent along with healthcare information
	7	(1) (3)	Clearly distinguishable, easily accessible form, using clear and plain language	If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Regulation shall not be binding. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.	Resource: Consent	Can not be used to capture consent! Use … instead … To implement this - use it in this way … Keep track on date when consent was withdrawn
					Vocabulary:	
	8	1	child's consent	Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.		
Transparency: The right for transparency requires to provide a lot of information about processing of personal data on request. This means you need to keep track of the processing of personal data. Information needed: • What category of personal data is processed for what purpose • Where did it come from based on which consent and for what purpose? • Where did it go to?	12		Transparency	The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, …. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. ...	-	While article 13 and 14 is about provinding general meta information to the data subject, the definitions in articles 15 to 20 require to keep track of the processing of personal data.
					Resource: AuditEvent	The AuditEvent resource can be used to track the source of an information. This includes …
	14	2f	Data that have not been obtained from the data subject	Provide the data subject with the information from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;	Resource: Provenance	The provenance can bei used to track the source of an information. Use Provenance resource instead of AuditEvent in case of … Furthermore provence can be used wherever a signature is needed.
	15		Right of Access	The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information: (a) the purposes of the processing; (b) the categories of personal data concerned; (c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations; ...	Security Labels	Use security labels to tag data with purpose of use
					Resource: AuditEvent	AuditEvent can be used to record all access/use/disclosure (FiveWs), so can inform a notification
					Vocabulary: PurposeOfUse vocabulary	Purpose of activity
					Vocabulary: Confidentiality classification	Categories of personal data confidentiality classification
					Vocabulary: Confidentiality classification	Categories of personal data sensitivity classification

	19		Notification of others	Any rectification or erasure of personal data or restriction of processing shall be communicated to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort.	Vocabulary: Confidentiality classification	
Right to erasure ('right to be forgotten')	17			Data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay. (under certain conditions)	Vocabulary: Confidentiality classification	possible gap: operation?
Portability: Patient can ask to get data in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller. Information need: • All healthcare information regarding observations	20		Right for portability	The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where ... THIS ONLY APPLIES when the processing is based on an"explicit consent"!	Vocabulary: Confidentiality classification	all resources. GAP: Open question: how to deal with data
General Security: Need for technical and organizational measures (TOM) to protect personal data.	32		Security of processing	Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate	Vocabulary: Confidentiality classification	Secure processing, secure transmission, authentication and authorization