Privacy and Patient Involvement in e-Health Worldwide: An International Analysis

Arno Appenzeller

Vision and Fusion Laboratory
Institute for Anthropomatics
Karlsruhe Institute of Technology (KIT), Germany
arno.appenzeller@kit.edu

Abstract

Nearly every nation is actively working on an e-Health policy or already has one. Personal Health Records (PHR) are considered as one of the key elements in the digitisation of the health sector. While nearly every e-Health agenda mentions privacy and data protection, the real world implementation can differ. A recent example is the planned launch of the German "Elektronische Patientenakte" (ePA), which has only limited data control features for the patient in its first version. This paper gives an overview of how the e-Health policies of the G7 nations handle patient involvement and privacy for their PHR projects. With this analysis we show that privacy and patient involvement are crucial for the acceptance of such projects. Finally we propose a data sovereignty framework with guidelines for PHRs to give a user control over his data and establish trust in such systems through broad access, fine granular control, informed decision making, intuitive user experience and comprehensible transparency.

1 Introduction

e-Health applications and their general use is becoming more and more common and widely available. Nearly every developed country has a national e-Health

strategy to make use of the data created during a patient's treatment. There are enormous expected benefits from the broad availability of electronic health data. From better data availability for medical research, paperless hospitals that can easily send data to a patient's general practitioner to patient centred care where a patient is in the middle of the treatment and is in possession and control of all data. While those are just examples it is clear that the potential benefits make e-Health projects worth to be pursued for a long time period. When looking at the German national e-Health project, the "Elektronische Patientenakte (ePA)", which is set to launch in 2021, it can be easily seen that patient involvement and privacy controls are controversial topics. To speed up the launch of the ePA there are several limitations to access right management for the patient in the initial version.[1] A fine granular access management is promised at a later time but with no concrete dates yet. This lead to a lot of controversy and discussion from several parties. The German Federal Commissioner for Data Protection and Freedom of Information Kelber announced that this violates the General Data Protection Regulation (GDPR) of the EU and that they will pursue legal checks before the ePA launches.[2] It remains to be seen if this will weaken public trust in the nationwide project. This is only one of the examples that shows that data sovereignty is an important topic when it comes to digital personal health records. According to GDPR Article 9, personal medical data is considered as sensitive data and must not be processed by default. To make processing of personal health data possible (or the other sensitive data, that is stated in Art. 9) one of the exclusions of Article 9 Paragraph 1 a) to j) must be fulfilled. One of these exclusions is the explicit declaration of consent to the data processing by the affected person. While there are different approaches to the term of data sovereignty, there is still no clear definition what it means regarding the processing of medical data. The previous example for Germany and the EU regulation gives a glimpse of what is considered important in the EU in those terms. However nearly every country's e-Health strategy includes a project similar to the German ePA. Many European countries also define their strategy

[1] https://www.heise.de/newsticker/meldung/Elektronische-Patientenakte-Datenhoheit-kommt-spaeter-4427379.html [Accessed 25 November 2020; In German]

[2] https://www.heise.de/news/Datenschutzbeauftragter-kuendigt-Massnahmen-gegen-Patientendatenschutzgesetz-an-4873642.html [Accessed 25 November 2020; In German]

with GDPR in mind, but it is interesting how other nations for example the US handle the topic of patient involvement, control and privacy of personal medical data. It is also important to analyse if the e-Health programs even have a patient centred approach or if the focus is more on the broad availability of the data for doctors and research. This paper will give an in-depth look on the e-Health strategies of the G7 nations and other examples. Building on this analysis of the different countries and especially the role of patient involvement and privacy in those programs, we will define criteria for data sovereignty for personal medical data. The paper is structured as follows: At first we will define the term data sovereignty and what it can mean for patient involvement. After this we will give an overview of e-Health in the G7 nations and other good examples. With the provided analysis of our findings, we will improve our data sovereignty definition and discuss our results. We close this paper with a conclusion and an outlook to further research, that is necessary in this area.

2 Data Sovereignty for Patient Involvement

The term data sovereignty is nowadays mostly used not only for personal data, but also for the processing of data as an economic good. However for both use-cases a wide range of control and possibilities to intervene is mandatory. When looking at the patient's perspective of data sovereignty, it is necessary to have a look at what existing regulations enable for the affected person. In the introduction it was already mentioned that the GDPR requires consent to process medical data. There are also some requirements for privacy consent in the GDPR. First every consent must have a specific purpose. Art. 5 Par. 1 b) says that a purpose has to be unambiguous and that the data is not allowed to be processed for something that is not consistent with the declared purpose. Furthermore the data should be limited to what is necessary for this purpose to enable data minimisation. Another requirement made in Art. 4 Par. 11 is that a consent should be freely given and express the affected person's explicit agreement to the data processing. Besides this it should be always possible for a subject to withdrawal its consent. Also the Recital 32 indicates that an opt-out principle for personal data is not allowed. So any pre-ticked boxes or the assumption, that

remaining silent means confirmation are not lawful. Finally the Article 15 of GDPR requires that a subject should have the right to access its data to see if data was processed and for what purpose it was done. It remains to be noted that while GDPR is a European regulation, the execution between countries can be different. For example Belgium explicitly requires written consent for the processing of medical data. Furthermore Belgium also requires direct access for the patients to their health data, while Portugal limits access to physicians. In Germany there are also specific laws and regulations that have implications on the execution on GDPR such as the local hospital regulations or the laws like the Patientendaten-Schutz Gesetz (PDSG) mentioned in the introduction. Even with the common GDPR the EU remains fragmented, which makes a closer look necessary [7]. In terms of digital consent the level of granularity is always an important topic. The best case would be an arbitrary level of granularity for consent. This means a patient could choose any data he wants to share with any third party the patient wishes. In reality those approaches are often limited. The limitations can have several reasons like technical limitations or limitations of user interfaces. The German law defines the basic control over personal data as information self-determination. While this term comes from an age before personal health records, the basic principles like control and transparency of data usage remains important. Therefore we consider data sovereignty as information self-determination + $\boldsymbol{X}$. While this $\boldsymbol{X}$ seems arbitrary it must be defined interdisciplinary. There are legal, ethical and technical considerations that needs to be done. For example not every legal definition can be executed in the exact same way technically and not every technical possibility comes without ethical concerns. However the technical side of data sovereignty has to enable everything needed in terms of consent, with a rich digital consent management, and transparency with possibilities to automatically track usage of personal health data. Nevertheless as described before technical solutions alone are not sufficient, therefore this paper gives an overview of the state of the art and suggests technical solutions that can help to improve data sovereignty.

3 e-Health in the G7 Nations

In this section we provide an overview of the e-Health projects in the G7 nations and other good examples. The overview will be focused on privacy and security aspects of the different projects.

3.1 Methodology

For our research we choose a qualitative approach. We focused on the G7 nations since that is where we expected the most resources available in English language versions. In addition we decided to include a few other notable examples we found during our research. For our systematic research approach, we used the directory of e-Health policies by the World Health Organization (WHO), which was created with information of the states itself or through an online search and research in academic literature [16]. The directory entry served as starting point for a general overview. In addition the European Union has a similar overview for a few selected nations [9]. For a more focused view on privacy policies regarding e-Health, we did our own literature and online research.

3.2 Germany

As mentioned in the introduction Germany has a lot of ongoing e-Health projects, but the largest is the national ePA, which is created by a consortium of different parties called gematik.[3] Data protection and privacy is a core topic while developing the ePA. This policy has a legal foundation in the so called e-Health law, which requires the highest priority for data protection from a legal and technical standpoint [2]. The gematik approach to fulfil this requirement is with the policy that no data should be accessed through the *public* internet and that a secure tunnel is required anytime [11]. Nowadays with the rise of mobile applications this approach is not fully valid anymore, since smartphone apps, that give access for a patient to his data, are planned. Besides this another

[3] `https://www.gematik.de`

use-case is data usage when visiting a doctor. Access to this data requires two factors from each party. One factor is the so called “Gesundheitskarte”, which is a chip card that is also proof of health insurance. When a patient wants to access his data, he also needs to enter a PIN code. In this scenario the doctor also needs to prove his/her identity and confirm access with his medical id card, which is similar to the “Gesundheitskarte”. In addition every access to data of the personal health record is recorded in a log file. This helps the patient to trace the usage of his data. In terms of patient control the ePA tries to do a staged rollout of control mechanism for the initial launch. In the first version only basic access control is possible. This means that a patient can give a doctor or a different party full access to every data or no access. This lead to a lot of controversy as described in the introduction of this paper. In addition the final planned stage will still lack the option of full control since access rights can only be managed for several document types like a doctor’s letter, that includes more than one medical observation and not a fine granular level for every medical resource of a patient. In 2014 Dehling et al. did an evaluation of the ePA project and compared it to their approach of patient-centred health information technology service [5]. They described several requirements on how sensitive medical information should be handled with a focus on privacy and security. Their result was that ePA was lacking a lot of things like the possibility for anonymous data sharing, unlinkability and some things like confidentiality, access control and authorisation are only partly fulfilled. It remains to be seen how well the German ePA will be accepted with all its privacy controversy, when it is set to launch in 2021.

3.3 France

France has several long term national e-Health strategies [8]. It is part of a digitisation agenda from 2011 where e-Health is a fundamental part. Inside this e-Health agenda there are five key points and privacy is one of them: “Open access to health data, respectful of personal information privacy, to serve the steering of the health care system, as well as public health and research (open data)” [13]. 2011 was also the year of the introduction of France’s first personal health record project, the so called Dossier Médical Personel (DMP). The main

principle of the DMP is not to be a complete health record of a patient, but rather an exchange and information platform where physicians can include the information from a patient they consider necessary. It is also a more document based platform that includes files like physician reports based on international standards like the Clinical Document Architecture (CDA). The whole DMP is opt-in and will be created by the general practitioner (GP) if a patient gives consent. In terms of patient involvement the DMP has an interesting history. After the initial launch only doctors were able to access a patient's DMP. There was no explicit way for a patient to access the records without a doctor. This caused a very low adaption of the platform, which lead to a relaunch that was more patient centred and provided direct access for the patient. With this higher adoption and acceptance was noticeable[3]. This version also included granular access right management for the patient. First a patient needs to authorise every physician, so that he can have access. Then every document can have a certain status. The status can be open so that everyone that has access to the DMP can access it. Another status is hidden, where only the patient, the physician that created the document and the GP see the resource. Other doctors see that there is a hidden file. Lastly there is a confidential status, which can be used when there is a sensitive diagnosis that should be viewed for the first time in the presence of the corresponding doctor. In addition to these access rights a patient can upload own documents and see an access log for every document.

3.4 Italy

Italy currently has no nationwide personal health record project with a focus on direct patient involvement. However there are different e-Health projects to introduce a nationwide electronic health record (EHR). The e-Health law sees three main tasks for an EHR: improvement of treatment, research and evaluation of the care quality. While there is no direct patient involvement, patients can control if there is an EHR and what data will be stored there with their consent. Besides from exceptions for patient care or treatment, the patient is in the center of the consent decision [1]. It needs to be mentioned that this is a legal requirement and the patient has no technical way to control this yet. In the past this lead to cases where EHRs were created without consent. Nevertheless

the patient has a right to get access to the EHR and privacy is a core principle in laws and strategies for e-Health. From a technical perspective there is still more to do to introduce the EHR and to improve direct patient involvement [10].

3.5 United Kingdom

The UK with its centralised National Health Service (NHS) launched several EHR systems in the past. In 2012 the government released a strategy paper that described a ten year framework for health and care [6]. Two key points were that the patient should be in the center of care and that digitisation should give benefits in a broad spectrum. This starts with tools for patients to make digital appointments, receive digital prescriptions and self-assessment tools. Furthermore standardised data communication allows data to improve the quality of care and reduction of inconsistent or incomplete data for health care providers. The strategy paper also described privacy concerns as potential issues. The paper stated the following position regarding those concerns: "not sharing information has the potential to do more harm than sharing it". However there are no more details besides that data should be shared in a confidential and private way and that patient should control this process. One of the already launched projects is the Care.data program.[4] The project aims to store all data of GPs in a common centralised database. Patients can deny consent to participate, however data will then be store anonymised. The focus of Care.data is on the secondary usage of data. Hoeksma took an in depth look at the program and its implications on privacy [12]. There is paid access to the platform and it offers matching of data from different sites to enable longitudinal tracking of patients' progress. This was done by using a patient identifier, the NHS number, date of birth, sex, ethnicity and postcode. After the linkage those identifiers are replaced by a pseudonym. Overall Hoeksma criticized the platform for its lack of transparency for the patient. All in all the missing transparency and other issues lead to the shutdown of the project. Another project that is still in use is the Summary Care Record. This service is a personal health record platform similar to the system of Germany's ePA. It is only created with the patient's consent, which can have

[4] `https://www.england.nhs.uk/2013/10/care-data/`

different levels. It is possible to consent to the storage of all information or only to allow the storage of necessary medical data. Currently the patient has no independent access to the platform, but can request the stored data from his GP. There are also some privacy concerns related to the service as the foundation medConfidential stated when they analysed conformance with the GDPR. [5] In addition there is access for secondary use for third parties. This is a default and needs explicit opt-out by the affected person. Like before the opt-out options have different stages. Opt-out can be universal or the patient can opt-out for every secondary use except when the explicit purpose is to provide his own treatment or care. The third-party access also lead to some controversy when life insurance or credit-card companies gained full access through subject access requests, that should only provide them the relevant data for the purpose.[6]

3.6 United States of America

The USA with its federal states has a variety of federal and national privacy laws, that lead according to Dumortier et al. to problems in regard of the introduction of e-Health [7]. Additionally many privacy laws are rather old and from a time before the digitisation. The major regulation in terms of health data is the Health Insurance Portability and Accountability Act (HIPAA), which has general privacy rules for personal health data. One of the main principles is that a patient must give his consent before health data is processed or given to another party. One exclusion is the usage in the context of a treatment or to process payment. However the patient should always have a certain degree of control for sensitive data. HIPAA also regulates when consent is needed and how a consent has to look like. It gives patients the right to access their data and the right to correct data. There are special requirements how to use data for secondary usage and who is allowed to do it. The HIPAA regulation is created to avoid that personal health data gets into the hands of unauthorised people. Besides privacy regulation HIPAA also has requirements in terms of

[5] `https://medconfidential.org`

[6] https://www.telegraph.co.uk/news/nhs/10855450/Probe-into-claims-that-insurers-given-access-to-full-medical-records.html [Accessed 25 November 2020]

security of the data. It remains to be noted that federal law can lead to exclusions and exceptions of the HIPAA regulation. This makes exchange of health data between federal states difficult. Besides national projects and strategic plans to boost the digitisation of the digital health sector, there is an existing solution called Blue Button.[7] This EHR service is created by the Blue Button initiative and is supported by many health providers on a voluntary basis. If there is a website that provides the possibility to safely download the personal health data of patients a blue button appears and enables the possibility to do so. The format does not necessarily have to be machine readable, it also can be a PDF or a some other document. Rather than providing a personal health record platform like in other nations, the intention is to make analogue exchange of health data easier and enable a possibility for the patient to get access to his data. There is also a successor in development called Blue Button+ that plans to enable a digital exchange with explicit control of the affected patient. In addition to the initiatives of the government there are many projects from private companies like Apple Health or Microsoft Health Vault to create personal health records.

3.7 Japan

Japan has a long history of the introduction of electronic health record systems. It already started in 1998 with the development of formats for the EHR. Those fundamental approaches had considerations about security but obviously did not look at patients in control of their data. There are regional differences in terms of e-Health usage. For example there are hospitals that offer their own EHR where patients have access but there is no nationwide personal health record. In 2018 the next-generation medical infrastructure law was introduced [15]. After a look at the status quo in terms of e-Health, which showed that only the minority of hospitals use EHR systems, that most of digital patient data remains unused and that documentation of patients' EHR is mostly incomplete, the new law allowed access to anonymised patient data for secondary usage like research without explicit consent of a patient. Nevertheless the patient will be informed about the usage of his data and can intervene - no intervention means consent.

[7] `https://www.healthit.gov/topic/health-it-initiatives/blue-button`

Most of the system and decisions how to use data remain in the responsibility of the participating hospitals. They need to decide how to anonymnize the data and if and how the patient should be involved. A study from Morris et al. showed that most of Japans population have privacy concerns and favor a system where they have control [14].

3.8 Canada

Canada has a privacy regulation called Personal Information Protection and Electronic Document Act (PIPEDA) similar to the HIPAA of the US. The goal is to protect personal health data from commercial usage without consent [4]. Furthermore there is Canada Infoway, which develops e-Health solutions for Canada.[8] A key goal is that the patient is in the center of the treatment. However there is currently no nationwide general personal health record.

3.9 Others

Besides the G7 nations there are other good examples for national e-Health initiatives with patient involvement. One example is Australia which has a system called My Health Record for a personal health record.[9] Privacy is a very strong requirement there and is enforced by law and technical requirements. Another example is Estonia, where there is one central platform where every health data is stored. In terms of privacy this project follows the rule of GDPR.

4 Analysis

When looking at the e-Health policies of the G7 nations and the role of privacy and patient involvement it becomes clear that nearly every nation applies some kind of general regulations like the GDPR or more health specific ones like HIPAA. In addition to those general regulations many nations have specific

[8] https://www.infoway-inforoute.ca/en/
[9] https://www.myhealthrecord.gov.au

laws for e-Health. For example Germany has a whole series with the recent PDSG as example. One interesting observation is that European countries have different executions of GDPR in terms of e-Health. Another observation is that there is a gap between technical execution and legal requirements. A good example where the technical planning is behind the law is the staged launch of the German ePA in terms of access control. A general impression is that nearly every personal health record is in an early phase. The DMP in France is a good example what impact patient involvement has on acceptance. This should be considered as cautionary example about how a good revamp with the patient in mind can look like. When looking at projects from the UK the importance of privacy can be shown by looking at projects cancelled due to privacy issues. Unfortunately there is no project that meets our requirement for data sovereignty in terms of data control and an arbitrary level of granularity to do so. The lack of complete data control is also related to open questions in terms of secondary usage and data donations. This is a very sensitive topic since there needs to be a fair trade off between data usage for research, which potentially benefits the general public in general and protecting data of individuals. The depth of this controversy can be easily seen by the discussion whether such processes should be opt-in or opt-out. With the general overview and some failed examples our research shows strong indications that it is important to involve the patient in a transparent way instead of hiding such data usage from him.

In general it is shown that technical solutions alone can only be partial solutions. Another major topic is to intuitively present the technical possibilities to the user through a suitable user experience. This should help the patient to be in the position to control his data, but also understand the implications of the control. To achieve this we propose a data sovereignty framework for personal health records that gives user control over his data and establishes trust in the system with the following properties.

- **Broad access:**
  Independent access is mandatory for every aspect a user needs for data sovereignty. Access should be as easy as using a dedicated app on the patient's smartphone. Access exclusively in presence of a physician should be discouraged because it will not let the user have an independent look on his data.

- **Fine granular control:**
  A user should be able to control every access to every datapoint of his PHR. When a consent for data usage is requested the user should be able to decide which data is allowed to be used by whom. This also leads to requirements for the underlying data structure. Documents that combine different data of patients should be avoided or also offer fine granular control.

- **Informed decision making:**
  Any decision which is not based on information or deeper knowledge can not be an informed decision. This property has consent decisions in mind, which can be very complex and hard to understand for a patient. A sovereign patient should be able to know what he does at any time. This should be supported by recommendation systems that evaluate decisions based on the patients preference. In the concrete case of consent this can be done by considering the preferences of the user, the requested data and the purpose of the request.

- **Intuitive User Experience:**
  All possibilities are limited when a user does not understand them. This is a rather interdisciplinary challenge from an ethical, legal, technical and design standpoint. For example an access system where the user feels overwhelmed by the possibilities will not help him to be sovereign. The mentioned discipline must define the requirements, so that the user has a good experience.

- **Comprehensible transparency:**
  A patient should be able to reproduce every usage of his data. He should not only be able to see the first data usage but also what such first data request imply, for example a research project that gives data to a partner to process it. This should be supported from a technical perspective and encouraged by guidelines how to use the data and make it transparent for the user.

We propose that a PHR that wants to enable patient involvement and data sovereignty follows those guidelines and execute and extend them according to the project's need.

5 Conclusion & Outlook

This paper gives an overview of privacy and patient involvement in e-Health worldwide. We see patient involvement, privacy and data control as crucial key points to enable data sovereignty in terms of PHRs. This term is defined by analysing the GDPR and how local policies extend it. We showed that data sovereignty requires more than what is demanded by current laws and their execution with the example of information self-determination, which is considered a fundamental right in Germany. From a technical point of view we see that this concept needs to be extended with a rich digital consent management and ways to enforce automatic data usage tracking for transparency. It has to be mentioned that the addition and extensions can not be purely technical and an interdisciplinary approach is required. Our overview looked at the e-Health policies of the G7 nations with a focus on privacy and patient involvement. The overview showed that while nearly every country has one or more laws that enforces privacy and patient involvement, the implementation is often limited. There are also clear examples proving that privacy and patient involvement is a key factor for the acceptance of a PHR. With those results we define a data sovereignty framework for PHRs. We propose that broad access, fine granular control, informed decision making, intuitive user experience and comprehensible transparency can help to give a user control over his data and establishes trust in the PHR system.

Our results show that more work is required in various fields to define a good framework for patient involvement and data sovereignty for PHRs. This should be done in an interdisciplinary effort. On the one hand there is the legal view. Further research and legislation is required to define the guidelines for the underlying technological possibilities of a PHR. In addition the ethical view should also be considered. Questions like what possibilities in terms of data control and privacy should be, if at all, limited for the patient need to be investigated. The issue when dealing with the trade off between usability and pre-filled decisions should be evaluated from an ethical point of view. Finally, besides the general technological implementation, there needs to be user research to create a proper user experience. This should investigate how a patient can be empowered, so he can understand his decision making and data control

without being overwhelmed by too many possibilities. Besides those open questions further observation of the current development in e-Health worldwide is necessary. One thing that could lead to new data on patient acceptance will be the upcoming launch of the German ePA. With a lot of controversy in terms of data protection and security, it remains to be seen how the compromises in those matters affect the adaption and acceptance of the project. While this is just one example of on-going digitisation, there will be more data and studies that could be used to refine our presented framework.

References

[1] S Bologna et al. “Electronic Health Record in Italy and Personal Data Protection.” In: *Eur J Health Law* 23.3 (2016), pp. 265–277.

[2] German Bundesrat. *German e-Health Law*. URL: http://dipbt.bundestag.de/dip21/brd/2015/0257-15.pdf.

[3] Philippe Burnel. “The introduction of electronic medical records in France: More progress during the second attempt”. In: *Health Policy* 122.9 (2018), pp. 937–940.

[4] Government of Canada. *Personal Information Protection and Electronic Documents Act*. URL: https://laws-lois.justice.gc.ca/ENG/ACTS/P-8.6/index.html.

[5] Tobias Dehling and Ali Sunyaev. “Secure provision of patient-centered health information technology services in public networks—leveraging security and privacy features provided by the German nationwide health information technology infrastructure”. In: *Electronic Markets* 24.2 (2014), pp. 89–99.

[6] Department of Health and Social Care. *The power of information: giving people control of the health and care information they need*. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/213689/dh_134205.pdf. Accessed 25 November 2020. 2012.

[7] Jos Dumortier and Griet Verhenneman. “Legal Regulation of Electronic Health Records: A Comparative Analysis of Europe and the US”. In: *eHealth: Legal, Ethical and Governance Challenges*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2013, pp. 25–56.

[8] European Commission. *e-Health: strategy and ongoing programs*. https://ec.europa.eu/health/sites/health/files/ehealth/docs/ev_20151123_co06_en.pdf. Accessed 25 November 2020. 2015.

[9] European Commission. *Overview of the national laws on electronic health records in the EU Member States*. https://ec.europa.eu/health/ehealth/projects/nationallaws_electronichealthrecords_de. Accessed 25 November 2020. 2016.

[10] European Commission. *Overview of the national laws on electronic health records in the EU Member States: National Report for Italy*. https://ec.europa.eu/health/sites/health/files/ehealth/docs/laws_italy_en.pdf. Accessed 25 November 2020. 2014.

[11] gematik. *Whitepaper Datenschutz*. https://www.gematik.de/fileadmin/user_upload/gematik/files/Publikationen/gematik_Whitepaper-Datenschutz_web_202009.pdf. Accessed 25 November 2020; In German. 2020.

[12] J Hoeksma. “The NHSs care.data scheme: what are the risks to privacy”. In: *BMJ* 348 (2014), g1547.

[13] Ministère de l’Économie des Finances et de la Relance. *France numérique 2012-2020*. https://www.economie.gouv.fr/files/files/import/2011_france_numerique_consultation/2011_francenumerique2020objectifs.pdf. Accessed 25 November 2020. 2011.

[14] K Morris et al. “Designing an Authorization System Based on Patient Privacy Preferences in Japan.” In: *Stud Health Technol Inform* 247 (2018), pp. 71–75.

[15] Otake, Tomoko. *Medical big data to be pooled for disease research and drug development in Japan*. https://www.japantimes.co.jp/news/2017/05/15/reference/medical-big-data-pooled-disease-research-drug-development-japan/. Accessed 25 November 2020. 2017.

[16] World Health Organization (WHO). *Directory of eHealth policies*. https://www.who.int/goe/policies/countries/en/. Accessed 25 November 2020. 2019.