

Bioethica

Vol 8, No 1 (2022)

Bioethica



E-Health Applications and Data Protection: a comparison of selected European Union members' national legal systems

Tatiana Ferreira

doi: [10.12681/bioeth.30545](https://doi.org/10.12681/bioeth.30545)



Copyright © 2022



This work is licensed under a [Creative Commons Attribution 4.0](https://creativecommons.org/licenses/by/4.0/).

To cite this article:

Ferreira, T. (2022). E-Health Applications and Data Protection: a comparison of selected European Union members' national legal systems. *Bioethica*, 8(1), 74–84. <https://doi.org/10.12681/bioeth.30545>

E-Health Applications and Data Protection: a comparison of selected European Union members' national legal systems

Tatiana Ferreira

Stagiaire, Hellenic National Commission for Bioethics & Technoethics

 pro.tatiana.ferreira@gmail.com

Abstract

In a context of constant evolutions and digitalization of the world, the health industry is one of the most relevant areas of innovation, especially with the development of countless types of electronic health (e-health) applications such as electronic health records or health applications on mobile devices. Furthermore, as data is becoming increasingly valuable, patients' health data, in particular, require the highest level of attention as it is vastly confidential and stored in massive amounts in e-health applications. Along with the development of new technologies, law is deemed to follow for regulating it. This implies that law must act as a protector for health data.

Within the European Union, the issue of data protection has been dealt with by the European Commission notably through the General Data Protection Act (GDPR) in 2018, but it is each country's responsibility to deal with new technologies in health, implement and apply data protection to health data.

Thus, it is relevant to compare how European countries deal with health data managing issues in e-health applications from a legal perspective and evaluate how efficient they are. For the purpose of this research, only three types of health applications will be compared as a sample, including electronic health records, electronic prescriptions and mobile health applications.

Keywords: data protection, e-health applications, health law, health data, cybersecurity.

Ηλεκτρονικές εφαρμογές υγείας και προστασία δεδομένων: σύγκριση των εθνικών νομικών συστημάτων επιλεγμένων κρατών- μελών της Ευρωπαϊκής Ένωσης

Tatiana Ferreira

Ασκούμενη, Εθνική Επιτροπή Βιοηθικής & Τεχνοηθικής

Abstract

Ο κλάδος της υγείας είναι ένας από τους πιο σημαντικούς τομείς καινοτομίας στην ψηφιοποίηση, ειδικά με την ανάπτυξη διάφορων τύπων ηλεκτρονικών εφαρμογών υγείας (e-health). Καθώς τα προσωπικά δεδομένα υγείας γίνονται όλο και πιο πολύτιμα, ειδικά τα δεδομένα υγείας των ασθενών απαιτούν αυξημένη προστασία, καθώς αφενός είναι ευαίσθητα και αφετέρου συγκροτούν μεγάλες συλλογές για την υποστήριξη ηλεκτρονικών εφαρμογών. Εντός της Ευρωπαϊκής Ένωσης, το θέμα της προστασίας δεδομένων έχει αντιμετωπιστεί, ιδίως μέσω του Γενικού Κανονισμού για την Προστασία Δεδομένων (GDPR) το 2018, αλλά αποτελεί ευθύνη κάθε κράτους-μέλους να εξειδικεύσει αυτή τη νομοθεσία ως προς εφαρμογές στον τομέα της υγείας. Επομένως, είναι σημαντικό να συγκρίνουμε πώς οι ευρωπαϊκές χώρες αντιμετωπίζουν ζητήματα διαχείρισης δεδομένων υγείας σε ηλεκτρονικές εφαρμογές, από νομική άποψη, και να αξιολογήσουμε πόσο αποτελεσματικές είναι οι σχετικές ρυθμίσεις. Για τους σκοπούς αυτής της έρευνας, μελετώνται οι πιο γνωστές εφαρμογές των ηλεκτρονικών αρχείων υγείας, των συστημάτων ηλεκτρονικής συνταγογράφησης και των εφαρμογών υγείας για κινητές συσκευές.

Λέξεις κλειδιά: προστασία δεδομένων, ηλεκτρονικές εφαρμογές υγείας, ιατρικό δίκαιο, ιατρικά δεδομένα, κυβερνοασφάλεια.

INTRODUCTION

If one should pick two things the recent COVID-19 pandemic has given attention to, all around the world, is the priority of public health and the significance of the digital transformation in a society. For example, the succession of lockdowns, social distancing policies and the emergence of contactless, virtual interaction has deeply changed our habits, especially in the area of healthcare. Health is a practice that inherently implies some form of human contact whether it be checking body conditions or practicing surgery. However, the development of technology, accelerated by the pandemic, has proven that these practices can be performed remotely as well as more efficiently, cost and time-saving.

In that sense, and since several decades, many States and in particular the European States have operated a change for more efficiency in their healthcare system. This change has been lifted by the innovations in digital health -coined as e-health or electronic health- and its generalization by means of implementation in the public healthcare sector.

E-health is a neologism that embodies how information and communication technologies (ICT) can be used to improve patients' health and the efficiency of the healthcare system as a whole. In other words, it refers to applying digital technology into healthcare practices. Thus, e-health is developed and implemented in society through various applications destined to be used by healthcare providers as well as by patients. These applications include, among others, electronic health records, e-prescriptions or mobile phone applications -that we will describe and analyze hereafter, but also remote surgery with near zero latency using 5G or remote consultations (as known as telemedicine).

However, health is among the most sensitive and protected aspects of the human life and digitalization means making available these information (data) on platforms where they could be used for unsolicited purposes, sold or even hacked and stolen. Trusting digital services always come with a risk, hence why laws, in the first place, has to guarantee a maximum protection for these information, presented in the form of health data. Thus, the key stakeholder in the development

of these applications is the protection of the individuals' personal data and their management by lawmakers in the European Union.

We will then analyze how the European Member States but also how the European Union (EU) deal with the use and protection of personal health data in their respective legal systems.

In the first place, it is relevant to present said e-health applications in order to identify the ethical and legal issues they present using three examples.

ELETRONIC HEALTH RECORDS

EHRs are defined by the European Commission's Recommendation on cross-border interoperability of electronic health record systems as "a comprehensive medical record or similar documentation of the past and present physical and mental state of health of an individual in electronic form, and providing for ready availability of these data for medical treatment and other closely related purposes".¹

According to the World's Health Organization, Electronic Health Records or EHRs are the primary hub of health data and its exchange through pharmacy and laboratory information systems. It is probably the most basic e-health application nowadays. Some even consider that the adoption rate of EHR systems is an important indicator of the degree of national e-health development². They are great tools for improving the quality, safety and efficiency of health systems.

It is the electronic version of a patient's health record that was historically created, used, and stored in a paper chart, though they are still

¹ Commission Recommendation of 2 July 2008 on cross-border interoperability of electronic health record systems (notified under document number C ((2008) 3282).

² Dameri, R. P.: Defining an evaluation framework for digital cities implementation. In Information Society (i-Society), 2012 International Conference on (pp. 466-470). IEEE (2012).

created, managed, and held by a healthcare organization and only healthcare professionals involved in a patient's care have access to it.

As for the content, an EHR may include a series of confidential data collected along a patient's lifetime concerning identification, demographics, medical and family history, previous hospitalizations, previous and current treatments, possible allergies and intolerance, diagnostic imaging as well as the results of laboratory and genetic tests. Different countries have different interpretation of what the content of an EHR should be and what data should be collected or not. For instance, the majority of EU countries (17 Member States) require that EHR must contain only health data (i.e data about their current or past health conditions or even organ donations in certain countries such as France or Bulgaria) apart from administrative information such as name and date of birth.³ EHRs that include non-health-related data can cover various personal information from professional activity to criminal offences.

It appears that a collection of such data implies very large and interoperable datasets that can be difficult to handle especially in terms of data protection.

E-PRESCRIPTIONS

E-prescription services are understood as the process of the electronic transfer of a prescription by a healthcare provider to any pharmacy for the retrieval of drugs by patients⁴. It

is seen as an alternative to prescribing on paper, with the general aim of full digitization of the prescriptions on the long-term. The use of this service aims at improving the efficiency in the healthcare systems as it can be used to digitally create and refill prescriptions for individual patients, manage their medication and keep track of their history, be connected to pharmacies and other drug dispensing sites and integrate the prescriptions into electronic medical records systems. E-prescription are also interoperable between healthcare professionals but it is also aimed to make them available all around Europe with the European Commission's eHealth Digital Service Infrastructure (eHDSI)⁵ project for patients to receive care anywhere in Europe.

What's more, this system is also used for its capacity of improving the safety of the healthcare systems in many areas including lowering the number of prescription forgeries, lessen the risks of errors or misinterpretations of prescription but most importantly regarding data protection, our main area of focus. The patient's personal medical data given by the prescriptions are encrypted, secure and can only be accessed with the patients' identification cards or number -for example- or by the professionals designated by said patient.

MOBILE HEALTH APPLICATIONS

Mobile health (mHealth) is a sub-segment of e-health and covers medical and public health practice using information and communication technologies. They are supported by mobile devices such as mobile phones, laptops, patient monitoring devices, personal digital assistants (PDAs), and other wireless devices. It especially includes the use of mobile communication devices for health and well-being services and information purposes as well as

³ Overview of the national laws on electronic health records in the EU Member States and their interaction with the provision of cross-border eHealth services Final report and recommendations Contract 2013 63 02, 23 July 2014
https://ec.europa.eu/health/sites/default/files/ehealth/docs/laws_report_recommendations_en.pdf.

⁴ eHealth Strategies, Country Brief: Finland Authors: P. Doupi, E. Renko, P. Hämäläinen, M. Mäkelä, S. Giest, J. Dumortier October 2010.

⁵https://ec.europa.eu/health/ehealth/electronic_crossborder_healthservices_en.

mobile health applications.⁶ Such applications vary from mobile teleconsultations, emergencies, health monitoring and surveillance, appointment reminders or even data sharing with healthcare professionals with over one hundred thousand different applications available nowadays.

Contrarily to the two former e-health applications mentioned *supra*, mobile health applications exclusively revolve around the patient and is designed for their use. This application contributes to the empowerment of patients. They allow them to manage their health more actively, live more independently thanks to self-assessment and monitoring of their own health.

Yet, m-health applications also benefit healthcare professionals in treating patients more efficiently as they become more aware of their health conditions and overall promote an adherence to a healthier lifestyle. Although, due its purpose of being controlled by non-professionals, it is important to bear in mind that this healthcare tool is not foolproof. In other words, the data collected from these apps can be unreliable because the patients might not use it well. Therefore, healthcare professionals should be careful while manipulating and sharing the data.

Indeed, due to their nature of being closest to the patients, stored on their phones which are part of the individuals' privacy, mHealth applications are particularly prone to collecting big amounts of data. Therefore, they need to be reliable on their use. Hence why the European Commission felt the need to establish The Privacy Code of Conduct on mobile health (mHealth) apps that aims to promote trust among users of mHealth apps⁷ covering privacy issues in order to gain the users' trust and following the GDPR.

LEGAL AND ETHICAL ISSUES

Nevertheless, such digital transformations undergone by European countries comes with a series of legal and ethical issues they must face including ensuring a good use of the collected health data and most importantly guaranteeing their security. It is particularly relevant to assess the advancement of health technologies in Northern European countries compared to the difficult progression of the South and the slow development of Western European countries.

NORTHERN EUROPE: FINLAND, DENMARK, SWEDEN, ESTONIA

In Denmark, Finland, and Sweden as well as Estonia, the State system was fundamental for the development of the information systems. The public model equalized the investments made for information technologies, in contrast with what occurred in other countries with a mixed contribution system. These countries have promoted EHR strategies and plans of action for e-health implementation ever since the beginning of the 1990s. Since then, they have been experts in Health ICT and the first to use these technologies in health services.

The Scandinavian systems are based on similar structures which are providing universal healthcare, maintaining healthcare in the public sector and using EHRs as the cornerstone of their healthcare model.

In order to assess the level of data protection for each country, it is important to assess the efficiency of their security systems and use of data in e-health applications.

In Denmark, the Danish Data Protection Act does not set out any provision on security requirements. Thus, the articles of the GDPR apply only. Data controllers and data processors must implement appropriate technical and organizational security measures necessary to protect data against accidental or unlawful destruction, loss or alteration and against unauthorized disclosure, abuse or other processing in violation of the provisions laid down in the Danish Data Protection Act. They benefit from a highly secured and efficient data protection scheme run by the Agency for Digitization (Digitaliseringsstyrelsen), involved in setting standards for health security such as the electronic mailbox system (e-Boks),

⁶ <https://ec.europa.eu/digital-single-market/en/mhealth>.

⁷ Privacy Code of Conduct on mobile health apps <https://ec.europa.eu/digital-single-market/en/privacy-code-conduct-mobile-health-apps>.

which is used by the health services for communicating with patients.

In Denmark, the development of e-health services was facilitated with the creation of the health portal Sundhed. It provides access to health information along with uses a system of engineering controls, such as encryption, electronic identification and control registers, in order to ensure privacy and the security of personal medical information. The problem with this platform is that there is excessive regulation regarding accessibility, thus it represents an obstacle for sharing health data, in particular EHRs.

Actually, because of its decentralized system, Denmark does not have nationwide electronic health records. This fragmentation in the e-health system prevents the country from reaching its full potential.⁸ With this issue, Denmark served as an example for the other countries who are still figuring out their digitization processes. It shows that even though interoperability initiatives are best managed on a regional level or by the authorities responsible for the provision of local health care services, cross-regional communication is essential during the initial phases of planning in order to set a common goal for countrywide harmonization, coherence and collaboration.⁹

Then, ranked sixth out of thirty-five European countries by the Euro Health Consumer Index¹⁰ for two years in a row, Finland boasts one of the most effective healthcare systems in the world in which digitization is one of the main preoccupations for improving healthcare efficiency. The security of data is organized nationally with the country-wide centralized

platform for e-health applications, Kanta, which also include data security policies and ensures data protection. Though, other data security policies, especially in the public sector may be applied. The Finnish Institute for Health and Welfare (THL) is responsible for the operative guidance of the information management in social welfare and health care. This guidance also includes data security policies for non-Kanta interoperable systems.¹¹

Though Finland has achieved a more widespread use of health information technologies than many other health systems, simply automating paper-based processes is not an optimal way of reaching efficient digitalization. Instead, digital health technologies should be used to enable and support key aspects of health care delivery such as coordination of services through efficient data sharing. In these respects, Finland still has much room for improvement.

Indeed, some even questioned the productivity of technologies such as the electronic medical record system which could be affected by rapid technological changes in technology, standards or even data protection requirements.¹² These compliance conditions in an ever-changing world generate financial issues since it can be very costly to keep all the systems up to date.

Though, similarly to the situation in Denmark, the development of health information systems has been largely uncoordinated at the national level, partly due to the decentralized healthcare system. As a result, several non-interoperable information systems are often used even within a single organization (for example within the same hospital), which seriously hinders

⁸ Kierkegaard, P. (2013) eHealth in Denmark: A Case Study. *Journal of Medical Systems*, 37 (6).

⁹ Patrick Kierkegaard, Interoperability after deployment: persistent challenges and regional strategies in Denmark, *International Journal for Quality in Health Care*, Volume 27, Issue 2, April 2015, Pages 147–153, <https://doi.org/10.1093/intqhc/mzv009>.

¹⁰ <https://healthpowerhouse.com/publications/>.

¹¹ [Information management in social welfare and health care - Information management in social welfare and health care - THL](#).

¹² Menachemi N, Collum TH. Benefits and drawbacks of electronic health record systems. *Risk Manag Healthc Policy*. 2011;4:47-55. <https://doi.org/10.2147/RMHP.S12985>.

the information exchange and data sharing across healthcare provider organizations. This inability to communicate coupled with the lack of information technology standards undermine the ability of the healthcare systems to take advantage of digitalization and efficiently store, share and secure their patients' personal data.¹³

As for data security, like other countries since the outbreak of the pandemic, Finland has been hit with a cyberattack on a hospital in 2020. This attack targeted to the most vulnerable, directly to patients, caused a shock in the country and its Nordic neighbors where the citizens started to question the safety of their data and their own laws.

Sweden is also part of the top performing countries in terms of e-health implementation, efficiency and data security. Though, Sweden does not benefit from national or regional measures to ensure quality standards and security of data and good use of e-health applications. Only the National Board on Health and Welfare issues guidelines on information processing to encourage health professionals to follow technical standards to ensure data security. The GDPR sets all standards in the country.

However, according to a 2016 report by the OECD¹⁴, Sweden still suffers from a fragmented data system in primary care which prevent effective data sharing. This is caused by a lack of central direction a large number of independent providers, leading to the development of multiple data systems used in primary care. Unfortunately, these systems are not always interoperable, which leads to a lack of data sharing across healthcare provider who do not receive necessary information to manage the patients, undermining their care. According to the report, only 20% of primary care doctors in Sweden are receiving necessary information to manage the patient within 48 hours

of discharge from hospital.

The issue in Sweden is investing in a standardized primary care information infrastructure to drive quality improvement, enhance interoperability and provide new opportunities for data sharing and co-ordination. Indeed, effective data sharing is important for data protection since it prevents mistakes, or loss of data.

It is very clear that Estonia is a model for e-health implementation developed incomparable technologies in the subject. This was the result of decades of investment and experimentation, and is actually about much more than technology. The key ingredient for the Estonian success story is trust. Estonians trusted their government to build a digital system that would serve and protect all of them. The 2007 cyberattacks in Estonia by the Russian government also acted as wake-up call, proving the importance of cybersecurity for the country as well as for the citizens.

Consequently, one of the crucial stakeholders for earning the citizens' trust was not only providing functioning and high quality (e)-health services but also guaranteeing their security and the protection of their health data in these applications. That's why, in Estonia, privacy is enshrined in a number of laws and regulations. Estonian citizens own and manage their personal data, including health data, and can check online who has looked at it. They are secure from any intrusion including public officials who cannot look at or use this data without reasonable justification. Citizens can also block access to their health data at any given time.

Though, as Estonia further improves, the government also keeps in mind the risks that come with digitization such as data theft and less control over the information flow. It is imperative to secure personal medical data at all times. The Estonian government banks on a ground-breaking blockchain technology to use in securing its citizens' medical data. The idea is that rather than

¹³ ["The Finnish Health Care System"](#) (PDF). SITRA. 2009. P.83.

¹⁴ [Health-Policy-in-Sweden-July-2016.pdf \(oecd.org\)](#).

storing and administrating data in a single database, multiple copies of the same data are synchronized in registers which are simultaneously updated and shared across a network of users.¹⁵ The aim of this system is ensuring the confidentiality, integrity and availability of data and assets and find a balance between these three components.

Though, regarding laws, the Estonian PDPA and the Implementation Act do not foresee any derogations nor additional requirements to the GDPR.

WESTERN EUROPE: FRANCE AND GERMANY

If Northern European countries are examples of success stories in e-health and data management efficiency, Germany and France also possess a solid potential for the implementation of e-health applications and overall digitalization of their healthcare systems. However, mediocre rankings in regulations, eHealth adoption by doctors and patients and the level of digitization in the healthcare system are discouraging factors for its success. It is then relevant to establish how well the digitalization is received in both countries especially in terms of data protection efficiency, trustworthiness, and quality of regulations.

In Germany, at national level, the most relevant legislations on health data include, for example measures for monitoring operations to ensure the security, availability, and usability of the Telematics Health infrastructure, a network aiming at exchanging health information. Each region has several data security policies regarding the standards. Germany also implemented data quality policies concerning the technical standards to be used to ensure the quality of health data for use in EHRs or other digital application.

Germany is the world's fourth largest healthcare market and ranked among the top ten in health expenditure per capita measured as a percentage of GDP. Nonetheless, Germany's healthcare system to date exhibits a comparatively low degree of digitalization. Regarding e-health in general, the first e-health-related law of German history has been passed in 2015. The law outlines a roadmap to build a nationwide digital infrastructure, aims to facilitate access to health information, and governs the introduction of new digital applications. It has allowed the implementation of new services such as remote consultation, emergency data storage, electronic medication plan and electronic physician's letter.

In the first place, it is relevant to report that even though Germany has good technical infrastructure and digital maturity, it is widely underused by the healthcare professionals. In 2019, 93% of doctors communicated with hospitals on paper, and less than half (a mere 44%) of all healthcare facilities (such as hospitals, outpatient medical practices, and medical centers) exchanged medical data by digital means. It appears clear that, even though the government puts work into developing infrastructures and adopting data protection laws and guidelines, data sharing and processing is very inefficient in Germany.

On the contrary, German patients are very accepting of e-health and are also very prone to using mobile health applications, especially since the coronavirus outbreak. Thus, there have been issues in the protection of data used by third parties in mHealth applications. Indeed, mHealth allows the collection of all kinds of health data and information about the physical activities of the individual who is wearing or using the device. If combined with other personal information and data from other sources, mHealth data plays a crucial role in building a digital image of the individual concerned. This draws conflicts between privacy and security. As an example, the personal health record app Vivy was launched in September 2018, it was strongly criticized barely 24 hours after it had been launched. Martin Kutzek, a freelance IT security expert from Karlsruhe wrote a blog post advising against the use of the Vivy app. He had discovered that the app transmitted data to third parties, in this case to tracking companies abroad, before the user even had the opportunity to

¹⁵ PWC, Estonia prescribes blockchain for healthcare data security, 16 March 2017, By Johnathon Marshall https://pwc.blogs.com/health_matters/2017/03/estonia-prescribes-blockchain-for-healthcare-data-security.html.

agree to the app's privacy policy. He pointed out that advertising and analytics modules have no place in apps that process highly sensitive information such as health data. He argued that even before the user has the opportunity to consent to the data protection declaration, a large amount of information is transmitted to third-party providers (tracking companies abroad).

In France, health data security is addressed by several bodies and institutions in France. The Agence du Numérique en Santé (ANS) elaborates an initiative policy with regards to security called General policy on the security of health information systems. This is rather a compilation of existing policies elaborated by several actors from the field of health.

What's more, following the implementation of e-health application, a 2019 ministerial ruling created the Platform on Health data, as known as "Health Data Hub" (HDH) in order to facilitate the health data sharing coming from any source including health insurances, hospitals, pharmacies etc. but also from e-health applications such as electronic health records or telemedicine. According to the Health Minister, it aims at organizing and value the health data collected in order to promote medical research as well as improve the French health system's efficiency. The creation of this hub also allows to develop more e-health applications using AI (artificial intelligence) which, using the collected data, would be able to predict a patient's health conditions and help with health diagnosis for personalized health services. Nonetheless, this project has been heavily criticized and raises concerns about data protection. Indeed, the project's report indicates that research is to be made transparent and the patients "will have the right to contest the use of their pseudonymized data" as indicated in the GDPR and the French Data Protection Law. It is also promised that the platform is a safe space for data collection, respecting the "sovereignty and independence" of the French health system to "foreign interests". The French DPA, CNIL, validated the project but issued three opinions (in 2019, 2020 and 2021) which bring to notice some concerns about the safety of the people's right and the protection of the collected data, especially due to the sensitive nature. These concerns are shared with the European Data Protection Board. They

issued warnings on the conditions of conservation of data and the modalities of access to the data as well as recommendation the data should be stored exclusively in entities submitted to the European Union's jurisdictions. This last point especially stirred a debate among politicians, healthcare practitioners, jurists and even the famous whistleblower Edward Snowden.¹⁶ He claims that France is giving up their data to Microsoft. Indeed, contrarily to the French DPA's recommendation, the data is stored in Microsoft Azure data centers claiming that they were the candidates with the best technology and offering the best security. Yet, in 2018, the US government passed a law called the Cloud Act which allows the US judiciary to access data stored in third countries and use it in criminal procedures. The risk of carrying this project appeared undeniably high, making the Minister's decisions incoherent.

Consequently, in April 2021, upon the recommendations of the CNIL, the government finally agreed to take actions to ensure the security of the data in the next two years. The Health Minister declared in front of the National Assembly the transfer of the data into French data centers or together with German infrastructures. The Ministry still declared in June 2020 that they are open for American investors to operate in France. This decision of letting two years pass before the change of infrastructures remains questionable regarding the data protection efficiency and security. Such delay allows the collection of data by foreign third-parties, increasing the cost of the operation and lose the patients' trust in the platform. A quicker change to European infrastructures would be much more profitable especially in these times of worldwide crisis in which health data becomes precious as gold.

¹⁶ <https://interhop.org/en/2020/04/30/le-gouvernement-contraint-les-hopitaux-a-abandonner-vos-donnees-chez-microsoft>.

Then, it is relevant to add that, like in Germany, the level of digitization in the healthcare system and the acceptance of the technology in France is relatively low and the development is slow. E-health applications such as e-prescriptions are still short from being used though mHealth applications tend to be more commonly used.

In conclusion, all these examples show the factors that contribute to making the system slow, inefficient, and sometimes even untrustworthy. The recent controversies regarding cyberattacks on hospitals also show that the authorities have to take actions to ensure the security and the efficiency of the protection of data in the healthcare sector.

SOUTHERN EUROPE: ITALY

As opposed to the aforementioned northern European countries, southern countries of the continent and especially Italy tend to be less inclined to invest into, develop and use electronic health applications. It is then relevant to understand how these health applications are implemented, used and how the health data are dealt with using the example of Italy.

Like most other countries, Italy relies on GDPR to harmonize all data privacy policies but no specific legislation addressing the processing of health data for providing digital health services has been adopted in the country. Italy is also armed with a Data protection authority, the Garante per la Protezione Dei Dati Personali, a partly-democratic institution made up of elected members. For instance, as for the security of the data collection and sharing in Italy, their Privacy Code does not prescribe any further security measures from the GDPR. However, additional safeguards for the processing of genetic, biometric data or data concerning health are issued by the Garante every two years. Additionally, the Privacy Code also does not set out additional rules on data breach security. However, the Garante is proactive in combatting this type of event. Recently, on February 19, 2021, the Garante gave a decision to fine a local health authority of Emilia-Romagna 50.000€ for not taking adequate measures for ensuring the security of personal data in the use of EHRs.

However, Italy is one of the countries in Europe which invests the least in healthcare. According to a recent OECD research, the Italian health expenditure is below the average of the other

countries belonging to the organization¹⁷. This lack of healthcare expenditure also discourages the investment in ICT technologies applied to the healthcare sector. It reflects the deficiency of shared vision of the digital innovation's profit and a lack of systematic investment in e-health. The system is commonly criticized for being incoherent. It is said that Italy "lacks an overall plan, a shared vision of e-Health. There are rules but there is no clear division of roles played by the state, regions and individual health authorities and hospitals. Indeed, although it is centrally financed, Italy's public health care system is managed regionally, therefore standards of care may vary and the best care is likely to be found in the north and center of the country, in cities such as Milan and Rome while the South is less developed. This situation contributes to the explosion of a lot of isolated investment, which is not integrated in a national system and is not sufficient to guide development of e-health in the country. In conclusion, the last decade has been dominated by two intertwined issues: regional fragmentation and the need to maintain financial control within regional health systems that prevents from developing the e-health scheme.

Nevertheless, amid the COVID-19 pandemic, Italy is actually experiencing a growth in digital health for developing e-health applications, mobile health applications in particular. For example, in late 2020, the Pittsburgh-based health system's international network UPMC has been awarded almost \$2 million to launch a telemedicine platform in Italy, which was hit hard by the coronavirus pandemic since its beginnings. Thus, the development of digital healthcare in the future

¹⁷ ICT Observatory in Healthcare: ICT in Healthcare: Why Digital Should Not Remain Only on the Agenda. School of Management of Milan Polytechnic Institute, Department of Management Engineering, May (2013). Italian Republic Ministry of Health: Electronic Healthcare File Guide.

could rely more on private initiatives than public investments which are too slow. Indeed, the representative for UMPC International in Italy added that “looking beyond the pandemic, this platform will create increasingly immediate and personalized health care in Italy.” However, if it’s good news for a better development, the collection, sharing and then protection of the sensitive data stored in these health applications might be problematic, especially since the aforementioned initiative comes from a non-European country which is not bound by the European Regulation (GDPR).

CONCLUSION

Last but not least it appears quite evident that, in order to establish strong ehealth applications, Member States must build and maintain strong centralized and mandatory foundations for eHealth through clear policies and strategies at national level. Though this could be a problem for traditionally or institutionally fragmented countries such as Italy, Spain or Germany especially since they also have to consider the other Member States for cross-border exchanges of data and other applications. Hence why, though national policies are a great base, the Scandinavian decentralized public health systems also work very well for implementing the technologies by giving local leaders more control and accountability to improve the e-health outcomes. Both actions from the national and local government then seem like the ideal model for implementing e-health and ensuring its efficiency as well as its security in terms of data sharing with strong national infrastructures. The preference of local level could be an efficient way to deal with the ethical issue of collecting, keeping and sharing such confident information like patients’ health data.

On the other hand, it is also essential for the governments to improve the security of the e-health systems and secure the health data to gain the people’s trust. Cyberattacks, self-serving third-parties and foreign interests are recurrent topics that further intimidate the populations in times when they are more and more aware of the importance of their personal data and especially their health data.

In the future, one of the main focus for e-

health applications development for EU Member States will be interoperability and cross-border exchange of health data at European level. Challenges are on how the national laws and the European framework must evolve to support cross-border e-Health services¹⁸ and ensure a high level of data protection beyond borders. It appears clear that the European Union is involved in this matter and makes the rule on their functioning, notably through enforcing the GDPR. European citizens are increasingly moving in and out of their countries and would benefit from similar levels of electronic health development and thus need the law on data security to follow their path as well as the development of technology in health.

¹⁸ The European Electronic Health Record. Critics and future, Pharmaceuticals Policy and Law, 2017, J. Valverde Lopez.