available at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Electronic health record: Wiring Europe's healthcare

Patrick Kierkegaard

Department of Computer Science, University of Copenhagen, Denmark

Keywords:
Electronic health record
Cross-border healthcare
Privacy
Access
Data protection

ABSTRACT

The European Commission wants to boost the digital economy by enabling all Europeans to have access to online medical records anywhere in Europe by 2020. With the newly enacted Directive 2011/24/EU on patients' rights in cross-border healthcare due for implementation by 2013, it is inevitable that a centralised European health record system will become a reality even before 2020. However, the concept of a centralised supranational central server raises concern about storing electronic medical records in a central location. The privacy threat posed by a supranational network is a key concern. Cross-border and Interoperable electronic health record systems make confidential data more easily and rapidly accessible to a wider audience and increase the risk that personal data concerning health could be accidentally exposed or easily distributed to unauthorised parties by enabling greater access to a compilation of the personal data concerning health, from different sources, and throughout a lifetime.

1. Introduction

Electronic health record (EHR) systems are becoming a reality in the western world. The paperless computerised medical record is creating a more effective and efficient system in the healthcare. The use of EHR is streamlining the industry by reducing labour costs, delay, pollution and medical errors. Clear, quickly available information results in unnecessary tests.

An Electronic Health Record is defined as "an evolving concept defined as a systematic collection of electronic health information about individual patients or populations. It is a record in digital format that is capable of being shared across different healthcare settings, by being embedded in network-connected enterprise-wide information systems. Such records may include a whole range of data in comprehensive or summary form, including demographics, medical history, medication and allergies, immunization status, laboratory test results, radiology images, vital signs, personal stats like age and weight, and billing information."[1]

An electronic health record is often used interchangeably with electronic medical record (EMR). However, these terms are completely different and should not be confused with each other. An electronic medical record contains the encounter information of patients in a care deliver organisation, while an electronic health record contains information from many or all care deliver organisations where the patient has been treated or has had an encounter. The EMR can be defined as the legal patient record created in hospitals and ambulatory environments that is the data source for the EHR.[2] One of the features of the EHR is the clinical database repository containing medical information about the patient, computerised entry for physicians, clinics and hospitals as well as pharmacies. These databases allow hospitals and physicians to exchange data information electronically with all entities within the health network including lab reports, radiology images and medical history.

Scandinavian countries have some of the most efficient patient-centred healthcare system with physicians using

[1] Gunter, T.D. and Terry, N.P., (2005). The Emergence of National Electronic Health Record Architectures in the United States and Australia: Models, Costs, and Questions in *J Med Internet Res* 7(1); http://emrguy.com/electronic-health-record/.

[2] Habib, J.L. EHRs, meaningful use, and a model EMR. *Drug Benefit Trends*. May 2010; 22(4):99–101.

0267-3649/$ – see front matter
doi:10.1016/j.clsr.2011.07.013

information technology to manage patient care. In Denmark, prescriptions, specialists' referrals, appointments, laboratory test results and electronic consultations are used by doctors to manage patient's care. This has been made possible through MedCom, a national centralised computer database which allows access to EMR information such as laboratory data, prescribing information, and communication between different health professional groups such as physicians and pharmacists. The Commonwealth Fund released a report on the usage of EMRs in Denmark. All primary care physicians (PCPs) use EMRs and 98% can manage their patients electronically. Usage went from 15% in the early 1990s to more than 90% by 2000. The keys to success are a coherent national policy, financial incentives to adopt health IT and technical support for providers, according to the report.[3] Virtually all primary care physicians have electronic medical records with full clinical functionality. Their systems are also connected to a national network, which allows them to electronically send and receive clinical data to and from consultant specialists, hospitals, pharmacies, and other healthcare providers. Under the auspices of MedCom, over 5 million clinical messages are transferred monthly. One of the most important innovations has been the "one-letter solution," which allows one electronic form to be used for all types of letters to and from primary care physicians; it is used in over 5000 health institutions with 50 different technology vendor systems.[4]

Patients also have the ability to electronically access all of their medical information including, medical records and test results through a website called Borger.dk. The website alerts the patient by email if a doctor, pharmacist or nurse views their records, and allows patients to make appointments, set end-of-life wishes, and even email their doctor for advice on illnesses that do not require an office visit. Residents of Denmark only need to log in using their Nem ID into the My Page section. They can retrieve information concerning their previous diagnosis, medications, laboratory tests, previous hospital stays, living wills and even organ donation.

In many of the Danish hospitals, doctors and nurses carry wireless hand-held computers to call up the medical records of each patient, including their prescription history and drug allergies. If a doctor prescribes a medication that may cause complications, the computer's alarm goes off.[5]

Denmark's ambitious healthcare IT projects over the last two decades are fully public-financed, and have cleared the way for these developments in EHR and telemedicine. The state has poured grants to support research in improving healthcare. One of the latest initiatives is the University of Copenhagen led initiative 'Co-Constructing IT and Healthcare (CITH)' together with the Technical University of Denmark, Copenhagen Business School, the IT University of Copenhagen and Rigshospitalet. The multifaceted research streams each focuses on special dimensions including information and security of the system. A software has been developed that will monitor the conditions of heart patients and improve exchange of information specifically for the patient, bioanalysts and doctor on a daily basis.

Odense University Hospital (OUH) is working to build a videoconferencing network on Denmark's existing healthcare IT infrastructure, which includes fully integrated EHR, ePrescribing, RIS and PACS, all on secure Internet protocols. Videoconferencing with patients is a reality at OUH and will be throughout the southern region of Denmark by the end of 2011. Telemedicine gives patients a new care experience, allowing them to receive treatment and consultation from their own home, while wearing their own clothes.[6] The aim of the project is to respond to closing hospitals and declining resources while offering an alternative to the traditional hospital visitation model.

The Integrated healthcare information system and telemedicine has put the small country at the forefront of effective eHealth. Other countries in Europe are still lagging behind with only limited EHR-like services operational at national level. The result is a patchwork pattern of eHealth use. The European Commission wants to boost the digital economy by enabling all Europeans to have access to online medical records anywhere in Europe by 2020. With the newly enacted Directive 2011/24/EU on Patients' Rights in cross-border healthcare due for implementation by 2013, it is inevitable that a centralised European health record system will become a reality even before 2020.

However, the concept of a centralised supranational central server raises concern about storing electronic medical records in a central location. The privacy threat posed by a supranational network is a key concern. Cross-border and Interoperable electronic health record systems make confidential data more easily and rapidly accessible to a wider audience and increases the risk that personal data concerning health could be accidentally exposed or easily distributed to unauthorised parties, by enabling greater access to a compilation of the personal data concerning health, from different sources, and throughout a lifetime.

2. Electronic health record in the EU

In 2008, an EHR IMPACT study was published by the European Commission, Directorate General Information Society and Media, Unit ICT for Health, and comprises of nine quantitative and two qualitative independent evaluations of good practice cases of interoperable electronic health record (EHR) and ePrescribing systems in Europe and beyond. The survey was conducted in 2007.

According to the study, almost all General Practitioner (GP) practices (87%) in the European Union use a computer with 69% of the EU27 GP practices having an Internet connection. Denmark, the Netherlands, Finland, Sweden and the UK emerge as the European frontrunners in eHealth use by

[3] http://articles.icmcc.org/2010/03/23/following-in-the-footsteps-of-fully-wired-denmark-physicians/.

[4] http://www.commonwealthfund.org/Content/Publications/Issue-Briefs/2010/Mar/Widespread-Adoption-of-Information-Technology-in-Primary-Care-Physician-Offices.aspx.

[5] Harrel, Ebben, (2009). In Denmark's Electronic Health Records Program, a Lesson for the U.S. Time Health at: http://www.time.com/time/health/article/0,8599,1891209,00.html#ixzz1SOXNNYAL.

[6] Chip Means (May 10, 2011) With telemedicine, Denmark puts patients first. Healthcare IT News. Available at: http://www.healthcareitnews.com/news/telemedicine-denmark-puts-patients-first.

General Practitioners. Greece, Latvia, Lithuania, Poland and Romania lag far behind. About 21% of European GP practices connect to other primary care actors, i.e. other GPs. Between the two types of connections to secondary health actors — hospitals and specialist practices — there is a noticeable gap. While about one-fifth of GP practices connect to hospitals, only somewhat more than one-tenth (12%) do the same with specialist practices. The most frequent connection is with laboratories with about 40% of the European GP practices connected while connection to pharmacies are considerably less frequent (used by about 7% of the practices). Electronic networks are also used for other professional purposes: 26% of the practices search for medication information, while 15% order their practice supplies online, 12% make appointments with other care providers and email exchange with patients is done by about 4%. Both telemonitoring and the transmission of vital data from patients' homes are virtually non-existent.[7] Administrative data are transferred to reimbursers by 15% and to other care providers by 10%. Medical data are transmitted to care providers or other professionals by 10%. Telehealth in Europe is mainly deployed in small local telehealth or telemedicine pilots, with increasing use of telemonitoring applications for chronically ill patients.

Only a few European countries have implemented a fully operational national primary care ePrescription service namely, Denmark (97%) followed by Sweden (81%) and the Netherlands (71%). The report concludes that Medical data exchange across national borders does not occur to any notable extent (0.7% on average).

3. EU strategy

The European Commission's Digital Agenda for Europe (DAE) is a flagship initiative of the EU 2020 strategy, which focuses on sustainable growth through ICT. eHealth is a key part of it. The DAE has launched major ehealth initiatives aimed at achieving interoperable ehealth systems across Europe, equip Europeans with secure online access to their medical health data by 2015 and achieve widespread deployment of telemedicine services by 2020. Telemedicine (also referred to as "telehealth" or "ehealth") allows healthcare professionals to evaluate, diagnose and treat patients in remote locations using telecommunications technology.[8] Telemedicine allows patients in remote locations to access medical expertise quickly, efficiently and without travel.

The EU Directive 2011/24/EU on the application of patients' rights in cross-border healthcare adopted on 28 February 2011 (also referred herein as the EU Cross-Border Health Directive) sets out for the first time the legal framework for eHealth in Europe, thus encouraging the development and adoption of electronic patient records throughout Europe.

The Smart Open Services (SOS) Project is a large-scale pilot intended to support the development of pan-European electronic patient records. SOS will focus on enabling the cross-border provision of ICT-based services that are already operational at national, regional or local level. The projects involves 12 member states and is intended to pave the way to pan-European, multi-lingual emergency patient records that will eventually link with national pharmacy systems.

Sharing patient's medical record between practitioners and healthcare providers is important to minimise the risk of complications. Optimal healthcare requires the availability of all necessary medical information in eliminating possible medical and administrative errors as what had happened in Germany. Lipobay is a statin drug used to lower cholesterol. The pharmaceutical industry has known for years that anti-cholesterol drugs impair the synthesis in the human body of the vital Coenzyme Q10 and cause renal failure, heart attack and muscle damage. The drug was prescribed to hundreds of patients by doctors and a number of patients died because of the effects of combining Lipobay with other medicines. This happened because doctors failed to crosscheck the medicines for each individual.

The Recommendation on cross-border interoperability of (EHR) systems was issued in 2008. It is the first EC document to set out the steps EU countries should take to establish compatible EHR system. The key objective is to allow patient choice to access his/her important information stored in electronic health record systems anywhere at anytime.

A Memorandum of Understanding (MoU) was signed on 17 December 2010 between the European Commission and the United States Department of Health and Human Services, which expresses an official willingness by the two parties to work together on compatible formats for EHRs (electronic health records). The MoU is intended to send a strong signal to all stakeholders that common standards and interoperability bring opportunities for a global approach for the benefit of patients, health systems and the market. Companies such as GE Healthcare, KP (Kaiser Permanente) and Verizon Business have been working to develop health record databases that can support interoperable record types.[9]

3.1. *Recommendation on cross-border interoperability of EHR systems*

Many EHR information systems store information in different formats creating difficulties in sharing patient data among health providers. Interoperability of electronic health record systems should make access easier, facilitate accurate data exchange, and enhance the quality and safety of patient care throughout the Community by providing patients and health professionals with relevant and up-to-date information while ensuring the highest standards of protection of personal data and confidentiality. Lack of interoperability of electronic health record systems is one of the major obstacles for realising the social and economic benefits of eHealth in the

[7] Alexander Dobrev, Marten Haesner, Tobias Hüsing, Werner B. Korte, Ingo Meyer, (2008). Benchmarking ICT Use among General Practitoners in Europe. Available at: http://ec.europa.eu/information_society/eeurope/i2010/docs/benchmarking/gp_survey_final_report.pdf.

[8] http://www.amdtelemedicine.com/telemedicine-resources/telemedicine-defined.html.

[9] Horowitz, B., (2011). U.S., Europe Sign Accord to Foster EHR Compatibility. EWeek Available at: http://www.eweek.com/c/a/Health-Care-IT/US-Europe-Sign-Accord-to-Foster-EHR-Compatibility-561574/.

Community. Development of fully functional interoperable EHR systems is a major challenge.

Market fragmentation in eHealth is aggravated by the lack of technical and semantic interoperability. The health information and communication systems and standards currently used in Member States are often incompatible and do not facilitate access to vital information for provision of safe and good quality healthcare across different Member States.

The Commission Recommendation of 2 July 2008 on cross-border interoperability of electronic health record systems (notified under document number C(2008) 3282) was adopted on 2 July 2008 and outlined the steps that Member States should take to establish an Electronic Health Records (EHR) system compatible with those in other Member States. The purpose of the Commission Recommendation is to contribute to development of overall European eHealth interoperability by the end of 2015.[10] The Recital states that the recommendation respects and observes the principles recognised by the Charter of Fundamental Rights of the European Union, in particular Article 7 on the right to respect for private and family life and Article 8 on the right of every individual to the protection of his or her personal data.

Electronic Health Record is defined as a means 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.

The Recommendation advocates the establishment of a comprehensive legal framework for interoperable electronic health record systems in Member States. Such a legal framework must recognise and address the sensitive nature of personal data concerning health and provide for specific and suitable safeguards so as to protect the fundamental right to protection of personal data of the individual concerned.

This legal framework should in particular:

(a) Analyse different personal data protection impacts of organisational alternatives for storing personal data concerning health and establish organisational structures for electronic health record systems in view of the specific risks for the rights and freedoms of data subjects, which best reflect the national, regional and local specifications and practices;
(b) Guarantee the patient's self-determination by allowing for the patient's autonomous and freely taken decision, supported by means of user-friendly technology, as to which personal data concerning health are to be stored and disclosed to whom in his or her electronic health record unless expressly required by national law. This decision shall be without prejudice to the possibility for the relevant healthcare body or doctor to store this data for treatment purposes;
(c) Establish that electronic health record systems are designed and selected in accordance with the aim of collecting, processing or using no personal data or as little personal data as possible. In particular, use is to be made of the possibilities for pseudonymisation or rendering persons anonymous, insofar as this is possible and the effort involved is reasonable in relation to the desired level of protection;
(d) Provide for an assessment of the information security risks and personal data protection impacts prior to the implementation of an electronic health record system, in view of the specific risks for the rights and freedoms of data subjects;
(e) Clarify the extent to which categories of personal data concerning health should be made available in electronic form or online. In particular, certain categories of personal data concerning health such as genetic or psychiatric data may have to be excluded from online processing altogether or at least be subject to especially strict access controls;
(f) Prescribe that processing of personal data in electronic health records and their systems must be required and carried out only by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person subject to an equivalent obligation of secrecy; ensure a reliable identification of patients and health professionals;
(g) Determine the conditions under which health data contained in electronic health record systems can be lawfully accessed and processed by persons other than the individual concerned, and for what predefined health purposes, including the security that should be assured while processing health data; specify these issues as policies that can be practically applied, technically implemented and enforced, inter alia, by the national data protection supervisory authorities;
(h) Ensure that patients are fully informed on the nature of the data and the structure of the electronic health record containing them. Patients should have alternative (conventional) means to access personal data concerning health related to him or her. In this context it is important to ensure that information provided to data subjects uses language and a layout that is easy to understand and is given in an appropriate manner to persons with special needs (e.g. children or elderly persons);
(i) Provide for special measures to prevent patients from being illegally induced to disclose their personal data contained in electronic health record systems;
(j) Make sure that any processing — especially the storage — of personal data in electronic health record systems takes place within jurisdictions applying Directive 95/46/EC or those with an adequate level of protection of personal data;
(k) Lay down detailed auditing requirements for the purpose of ensuring compliance with data protection obligations, such as reliable system of electronic identification and authentication, data access logging, documentation of all processing steps, duration of maintaining the auditing information, effective back-up and recovery systems, and enforce the adoption of these requirements or solutions according to best practices for information handling;
(l) Guarantee the confidentiality of electronic health record systems as well as provide for appropriate technical and organisational measures, including rules on incident

[10] Full text of Recommendation available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32008H0594:EN:NOT.

detection and management processes, in case of a breach of security or identity mechanisms leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed in electronic health record systems. Incidents or violations should be identified promptly and effectively and measures or solutions should be put in place to manage such incidents, including informing and involving the individuals concerned, the national data protection supervisory authorities, and other appropriate stakeholders.

Member States are also urged to stimulate the deployment of security-enhancing products, processes and services to prevent and fight identity theft and other privacy-intrusive attacks and to ensure that data protection safeguards are embedded in electronic health record systems, including through the widest possible use of Privacy Enhancing Technologies (PETs) in their design and implementation.

3.2. *The EU Directive on patients' rights in cross-border healthcare*

The EU Cross-Border Health Care Directive 2011/24/EU[11] establishes very firmly the right of EU citizens to seek healthcare in other member states. When wanting to go in another Member State, in particular to access diagnostic expertise, this access can no longer be denied and, at the very minimum, Member States will have to justify why. In general, the view is that citizens prefer to get treatment in their home member state, but if this is not possible and treatment is available in another member state, then this Directive firmly establishes that the citizen can access this healthcare and have the costs reimbursed by the home member state public health system. This means that the patient has to advance the payment. The Directive states that the home member state will pay costs up to the amount which the treatment would have cost under the home member state's public health system. This has been placed on the cross-border healthcare directive as a means to prevent health tourism. Instead of reimbursing the patient, member states of affiliation may also decide to pay the healthcare provider directly.

For overriding reasons of general interest (such as planning requirements for ensuring permanent access to a balanced range of high-quality treatment or the wish to control costs and to avoid any waste of resources) a member state of affiliation may limit the application of the rules on reimbursement for cross-border healthcare. Prior authorisation systems (where a patient makes a request to be treated abroad before they obtain treatment) may only be introduced for healthcare which is subject to planning requirements, such as hospital care (defined as care involving overnight hospital accommodation), healthcare that involves highly specialised and cost-intensive medical infrastructure or equipment, healthcare that involves treatments presenting a particular risk for the patient or the population, or healthcare which would be provided by a healthcare provider which could raise serious concerns with regard to the quality or safety of the care. A member state of affiliation may refuse to grant prior authorisation

- if the patient seeking cross-border healthcare will be exposed to an unacceptable safety risk,
- if the general public will be exposed to a substantial safety hazard,
- and if the healthcare is to be provided by a healthcare provider that raises serious concerns relating to compliance with standards and guidelines on quality and safety,
- or if the healthcare can be provided on its territory within a medically justifiable time-limit.

However, these exemptions are vague and some countries could use the limitations to reject prior authorisation.

As a general rule, if a product is authorised to be marketed on its territory, a member state must ensure that prescriptions issued for such a product in another member state can be dispensed in its territory in compliance with its national legislation. Sales of medicinal products and medical devices via internet, long-term care services provided in residential homes and the access and allocation of organs for the purpose of transplantation fall outside the scope of the directive.

The fundamental rights to privacy with respect to the processing of personal data in the cross-border healthcare is protected with national measures implementing Union provisions on the protection of personal data, in particular Directives 95/46/EC and 2002/58/EC.

The cross-border provision of the new Directive will deploy the application of ehealth and telemedicine involving exchange of electronic health data, remote monitoring and diagnosis, teleconsultation, electronic prescription and electronic referral. Improving the conditions for cross-border healthcare will be to the benefit of the citizens. However, it will at the same time embody certain risks for the citizens. The cross-border exchange of health data increases the risk of inaccurate or illegitimate data processing.

Technological developments in cross-border provision of healthcare through the use of ICTs using different incompatible formats and standards for the provision of healthcare may be an obstacle to cross-border healthcare provisions and cause possible additional risks to health protection. Variation in privacy regulations and data protection rules results in the fact that it is difficult to share patient records and other information between healthcare providers, regulatory bodies in the member states. For example, in Germany, there is strict division between the ambulatory and hospital sector. Data Protection Officers do not allow the flow of patient data in cross-sectoral care process. This is only allowed provided that there is an integrated care contract between the hospital and general practitioner. German physicians cannot have access to information gathered elsewhere-even in hospital- even if the patient has given his consent.[12] In contrast, Denmark allows the general practitioner access to his patient's record.

[11] Full Text of the Directive available at: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:088:0045:0065:EN:PDF.

[12] European Coordination Committee of the Radiological, electromedical and Healthcare IT Industry, (2011). Brussels. Available at: http://www.cocir.org/uploads/documents/10-1138-cocir_contribution_to_the_communication_on_personal_data_protection_in_the_eu.pdf.

The existing diversity of the Member States' health systems, specifically the different security levels applied by the Member States, easier and more widespread access to sensitive information, and the application of data for statistical purposes, gives rise to privacy concerns and possible misuse of medical information.

4. Data protection and EHR

The European Union is based on the respect for fundamental rights. Article 8 of the Charter of Fundamental Rights of the European Union and Article 8 of the European Convention for the Protection of Human Right expressly recognizes the fundamental right to the protection of personal data. With the entry into force of the Lisbon Treaty, the protection of personal data has become a fundamental right of the EU. More definite rules are provided by the Data Protection Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regards to the processing of personal data and on the free movement of such data were adopted on 24 October 1995 and Directive 2009/136/EC amending Directive 2002/58/EC (Privacy Directive) concerning the processing of personal data and the protection of privacy in the electronic communications sector and the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108).

The definition of personal data contained in Article 2 (a) of Directive 95/46/EC states:

> "*Personal data shall mean any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity*".

The Data Protection Directive 95/46/EC does not include an explicit definition of health data. However, Article 8 (1) of the Directive prohibits *"the processing of personal data revealing racial or* ethnic *origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning* ***health*** *or sex life."*

In *Bodil Lindqvist* (Case C-101/01), the ECJ ruled that in the light of the purpose of the directive, the expression 'data concerning health' used in Article 8(1) thereof must be given a wide interpretation so as to include information concerning all aspects, both physical and mental, of the health of an individual. Reference to the fact that an individual has injured her foot and is on half-time on medical grounds constitutes personal data concerning health within the meaning of Article 8(1) of Directive 95/46.[13]

Thus all data in medical records are considered as sensitive data and subject to the special data protection provisions in Article 8 of the Data Protection Directive. Additionally, the Cross-Border Health Care Directive defines 'medical records' as all the documents containing data, assessments and information of any kind on a patient's situation and clinical development throughout the care process. This would include any personal and administrative data contained in the medical document which has a clear and close link with the description of the health status of a person, such as date of admission to the hospital, invoices (etc.), according to Article 8 of the Data Protection Directive.

There are exemptions to the general prohibition of processing medical data.

(a) The data subject has given his explicit consent to the processing of those data (Art. 8 (2) (a). This means that 'general agreement' of the data subject e.g. to the collection of his medical data for an EHR and to subsequent transfers of these medical data of the past and of the future to health professionals involved in treatment would not constitute consent in the terms of Article 2 (h) of the Directive."[14] The consent must be genuine free choice after the data subject has received accurate and full information of all relevant issues in a clear and understandable manner. Moreover, Member State law can determine that in certain cases even consent of the data subject cannot lift the prohibition. Opt-out solutions will not meet the requirement of being 'explicit'. Mere silence or inaction (opt-out) typically will not be viewed as valid consent, especially in an online context. However, there is often 'implicit consent' about data, because there are multiple legal entities involved in providing care, different contexts and different persons, and no uniform approach.

Consent must be given prior to the data processing, after providing notice in a clear and understandable language to the data subject. Healthcare providers may pressure often clueless patients for consent regarding medical procedures and use of their data. Hence it is important that patients should be given information about the following, among other things: 1) the purpose for which their health information are to be processed, 2) disclosure of information to third parties, and 3) any transfers of information outside the EU.

In a recent case, Sweden's data protection authority ruled that a hospital's failure to provide patients with the choice to opt-out of the sharing of their medical and other data via an electronic health records system violated the law. The Data Inspection Board ruled April 18, 2011 that the sharing of patient records requires consent by the Patient Data Law, and that Stockholm's Karolinska University Hospital's method of consent did not meet those requirements. The hospital belongs to a data-sharing network that allows database access to both public- and private-sector healthcare providers.[15]

[13] Text of the Judgement available at: http://curia.europa.eu/jurisp/cgi-bin/gettext.pl?lang=en&num=79968893C19010101&doc=T&ouvert=T&seance=ARRET.

[14] Article 29 Working Party Working Document on the processing of personal data relating to health in electronic health records (2007). Available at: http://www.garanteprivacy.it/garante/document?ID=1386451.

[15] http://privacynewshighlights.wordpress.com/; http://www.datainspektionen.se/Documents/beslut/2011-04-19-karolinska-sjukhuset.pdf.

(b) Processing of the sensitive data is also allowed when it is necessary to protect the vital interests of the data subject or of another person in situations where the data subject is physically or legally incapable of giving his consent. This would include life or death situations e.g. the data subject is for example in comatose conditions. Article 8(2) (c) of the directive.

(c) Article 8(3) allows the processing of data for the **specific** purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of healthcare services, and where those data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of **professional secrecy** or by another person also subject to an equivalent obligation of secrecy.

According to the Article 29 Working Party, these derogations do not cover further processing which is not required for the direct provision of such services, such as medical research, the subsequent reimbursement of costs by a sickness insurance scheme or the pursuit of pecuniary claims. Equally outside the scope of application of Article 8 (3) are some other processing operations in areas such as public health and social protection, especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system.[16]

(d) Article 8 (4) of the Directive allows the Member States to derogate further from the prohibition of processing sensitive categories of data:

Subject to the provision of suitable safeguards, Member States may, for reasons of substantial public interest, lay down exemptions in addition to those laid down in paragraph 2 either by national law or by decision of the supervisory authority."

Processing of sensitive personal data must be justified by reasons of **substantial public interest such as "**public health and social protection – especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system – scientific research and government statistics (Recital 34 of the Directive).

The States also have a positive obligation under Article 8 § 1 of the Convention for the Protection of Human Rights and Fundamental Freedoms to ensure respect for the applicant's private life. In *I v Finland*, (20511/03), the European Court of Human Rights found against Finland and ruled that a person's right to respect for their private life (under the ECHR,) may be breached where the State *fails to take appropriate steps to secure data, so that it cannot be accessed improperly*. The applicant's private medical records were accessed by the other people (as a result of which she possibly lost her job as a nurse). The access was not recorded, as there were no records of this at the time. The Court decided that as the hospital was controlled by the State, Finland was responsible for the actions there. The ECHR found that if personal data is not secured adequately, and the State does not take positive steps to do so (and not just legislation but technical and procedural steps as well), then the state is in breach of Article 8.

The Court also emphasized the importance of confidentiality:

The protection of personal data, in particular medical data, is of fundamental importance to a person's enjoyment of his or her right to respect for private and family life as guaranteed by Article 8 of the Convention. Respecting the confidentiality of health data is a vital principle in the legal systems of all the Contracting Parties to the Convention. It is crucial not only to respect the sense of privacy of a patient but also to preserve his or her confidence in the medical profession and in the health services in general. The above considerations are especially valid as regards protection of the confidentiality of information about a person's HIV infection, given the sensitive issues surrounding this disease. The domestic law must afford appropriate safeguards to prevent any such communication or disclosure of personal health data as may be inconsistent with the guarantees in Article 8 of the Convention (see Z v. Finland, judgment of25 February 1997, Reports of Judgments and Decisions, 1997-I, §§ 95–96).[17]

From early times, the medical profession has taken the Hippocratic Oath which states "whatsoever I shall see or hear in the course of my dealings with me, if it be what should not be published abroad, I will never divulge, holding such things as holy secret." Patients' medical records should be made secure and should not be subject to data abuse by healthcare providers.

5. Privacy and security

European healthcare is threatened by soaring costs and limited resources. eHealth and telemedicine could support health systems transformation to respond to the challenges of demographic ageing, scarcity of resources, shortage of health professionals, the increase in chronic diseases by enhancing the provision of timely and appropriate healthcare for all and the more effective use of services and capacities in the health sector. Major advances in technology have allowed many new procedures and methods of diagnosis and treatment. The new feature is that a physician is able to see and examine a patient sitting on the other side of the globe. Information technology has developed telemedicine into a means of removing many of the limitations that stem from the distance to the patient. Simultaneous two-way sound, data and picture communication (interactive video) provides a far better basis for health professionals to give help aided, for example, by sight and with minimum delay. Devices such as hand-held computers are used record a patient's medical history. Information on

[16] Article 29 Working Party Working Document on the processing of personal data relating to health in electronic health records (2007). Available at: http://www.garanteprivacy.it/garante/document?ID=1386451.

[17] Text of Judgement available at: http://www.whereisyourdata.co.uk/whereismydata/wp-content/uploads/2008/08/case-of-i-v-finland.pdf.

vital signs and orders for tests are transferred electronically to a main database. More healthcare providers are using real-time medical equipment tracking systems, such as RFID, for patient identification, location and medication administration. Invasive personal health systems for illness prevention and/or for health status monitoring of patients include systems based on flexible and smart technologies adaptable to the human body and integrating the possibilities of electrical, optical, chemical, & mechanical sensors. There are, for example, RFID implants injected under the skin or attached to people to locate patients. These systems monitor various parameters (bio-signals, location, etc.), and when needed, communicate securely with health professionals as well as with intelligent support systems.[18] In the Netherlands, one of the areas that seem to be exceptionally well developed is the use of hand-held computers for electronic case management. After data are collected, it can be immediately transferred, using dial-up networking capacity, from the point of care to the central home care database. Records are regularly updated and are available to different health professionals within the continuum of care.[19] In Denmark, telemedicine is also impressive: high risk patients (diabetics and those using blood thinners) are being monitored in their own homes. If a patient has foot ulcers, the specialist nurse visitor uses a secure video link to discuss their current state with a doctor and decide on treatment. Patients taking blood thinners are also monitored; if the doctor assesses a risk of clots or haemorrhage, the patient is alerted and advised. A study to assess the potential of home monitoring for COPD patients is also underway. The patient uses a blue-tooth enabled pulse oximeter and spirometer during a videoconference with the doctor, who can then decide whether a nebuliser, oxygen, or other treatments are needed.[20]

With the opportunities and benefits that accompany the development of ICT come new risks, particularly for the privacy and protection of personal data of individuals. According to a recent study by the Identity Theft Resource Center, data breaches in the healthcare sector are occurring at a higher rate than in other industries[21] The increase may be due to the many different types of workers that have access to areas in healthcare organizations buildings where sensitive data is stored.

5.1. *Data breaches*

The concept of a centralised supranational/national central server raises concern about storing electronic medical records in a central location. The healthcare sector is as an area of high risk. There is a considerable risk of losing all of the data if the centralised system is destroyed from virus infections or other causes. Furthermore, hackers may gain access to the files for economic purposes or modify the patient's information. In 2010, despite being behind a firewall, and on a countywide anti-virus platform, a computer virus took out Bakersfield, California-based Kern Medical Center's HIS. This sent workers scrambling for paper records to keep the healthcare flowing. The hospital believed it was protected from Internet attack until cyber-attack penetrated its security. A lapse of judgment by a single employee cost the hospital 16 days of agonizing recovery from a particularly vicious attack. The hackers stuffed porn into the hospital's computers, forced hospital printers to continuously print until they ran out of paper, and eventually shut down a number of the Kern Medical Center's systems.[22]

Besides gaining access to hospital information systems, viruses can now infect clinical monitoring devices, networked devices used by medical personnel such as ipads used by doctors and nurses and even *surgically implanted electronic devices*!

According to a report issued by the eHealth Vulnerability Reporting Program (eHVRP), a collaborative of healthcare industry practitioners and technology providers formed to assess the security of the nation's electronic health records, there was not one system they could not penetrate.[23] In fact, banking systems have better and more elaborate systems to thwart hacking attacks. In 2009, hackers broke into a Virginia state Website used by pharmacists to track prescription drug abuse. They deleted records on more than 8 million patients and replaced the site's homepage with a ransom note demanding $10 million for the return of the records.[24] In October 2008, Express Scripts, one of the nation's largest processors of pharmacy prescriptions, disclosed that extortionists were threatening to disclose personal and medical information on millions of Americans if the company failed to meet payment demands.[25]

Due to the large amount of very sensitive private data stored on doctors' and nurses' laptops, which are often unencrypted, there is high risk for exposure or leaks. Policies and procedures may be in place, but often they are not followed. Once sensitive information is released causing damage to the person, the information cannot be secret again.

The National Health System (NHS) was responsible for almost one-third of all recorded data breaches in the United Kingdom for the last three years. The health service holds some of the most sensitive personal information of any sector

[18] Work Programme (2002). CORDIS. Available at: http://cordis.europa.eu/ist/bwp-en3.htm.

[19] Office of Health and the Information Highway (1998). Available at: http://www.hc-sc.gc.ca/hcs-sss/pubs/ehealth-esante/1998-tele-int/index-eng.php#ack.

[20] Denmark's Healthcare (2009). European Hospital. Available at: http://www.european-hospital.com/en/article/6086-Denmark%25C2%2592s_healthcare.html.

[21] http://www.idtheftcenter.org/index.html.

[22] McBride, M., (2011). Cyber-Attacks against Internet-Enabled Medical Devices are New Threat to Clinical Pathology Laboratories. Dark Daily. Available at: http://www.darkdaily.com/cyber-attacks-against-internet-enabled-medical-devices-are-new-threat-to-clinical-pathology-laboratories-215.

[23] Tucci, Linda (2007). Electronic medical records at risk of being hacked, report warns available at: http://searchcio.techtarget.com/news/1273006/Electronic-medical-records-at-risk-of-being-hacked-report-warns.

[24] http://wikileaks.org/wiki/Over_8M_Virginian_patient_records_held_to_ransom,_30_Apr_2009; FBI probes hackers $10 million ransom demand for stolen Virginia Medical Records (2009). Fox News at: http://www.foxnews.com/story/0,2933,519187,00.html.

[25] Krebs, B., (2008). Extortionists Target Major Pharmacy Processor. Washington Post. Available at: http://voices.washingtonpost.com/securityfix/2008/11/extortionists_target_major_pha.html.

in the UK. Of the NHS's 305 breaches, 116 data breaches were caused by stolen data and hardware. A further 87 were caused by lost data and hardware. The NHS was also not helped by the fact that 43 breaches were due to data being disclosed in error. The Information Commissioners Office (ICO) also said that 17 NHS breaches came from information that was lost in transit, 17 from technical/procedural failure, 13 from non-secure disposal, and 12 from 'other' causes.[26]

Human error is behind a high proportion of security breaches. In 2011, researchers for London Health Programmes revealed that they had lost unencrypted records of 8.63 million NHS patients.[27] More recently, a laptop containing names, addresses and medical information was stolen from Asperger's Children and Carers Together (ACCT). The hard-drive stolen from the charity's office included information about past criminal and child protection issues of the young people as well their names and addresses.[28] Freedom of Information (FoI) requests sent by the Yorkshire Postto trusts and other public organisations across Yorkshire revealed a number of serious data breaches, including a doctor accessing a colleague's medical records at a hospital in Doncaster, and a cleaner at a Rotherham hospital viewing a friend's private medical files. Other instance involved a receptionist at a hospital in Sheffield, who collected patients' personal contact records and used them for a second job as a market researcher. One of the worst offending trusts was Doncaster and Bassetlaw Hospitals trust. One case involved a nurse accessing the private medical test results of her child's father, while another incident led to a clerk receiving a written warning after looking up her brother's test results. Doncaster and Bassetlaw was unavailable for comment. There were also five incidents at Sheffield Teaching Hospitals which ranged from a staff member accessing information so that they could send a card to a relative, to staff looking through at a record of an ex-partner's new partner.[29]

In the Netherlands, the information that emergency services such as ambulances sends to one another, was transmitted unencrypted. Because the C2000 system in Brabant (a Dutch province) did not have full coverage, emergency services used P2000 instead, which sends unanonymized data: name, address, ailment etc. In one case, information was put online containing the information of a suicide attempt gone wrong.[30] The District Psychiatric Service in The Hague – which keeps the psychiatric and criminal records of (former) detainees, dumped a box full of such records **on the street**, together with 'other garbage'. A passer-by found the box and reported the matter to the Dutch privacy authority (CPB). This was in January 2010. The CPB has now reported about the case and discovered that for years, all medical and criminal files of detainees were stored in an unprotected cellar. The CPB reminded the Department of Justice that records like these are highly sensitive data and merit strong protection.[31]

In Spain, one in three Spanish hospitals is in breach of the Data Protection law. Spain has a data protection law (Ley de Protección de Datos) and a data protection agency (La Agencia Española de Protección de Datos – AEPD). A recent survey was conducted on the state of patient information security in Spain, and things look pretty grim. 40% of state hospitals, and 15% of private ones, have no register to record access to clinical files, and 45% do not include the standard legal wording on their forms which explains how and why patients' data is stored. Some 30% of public hospitals have no measures in place to prevent the loss of, or unauthorised access to, patients' data during transport or whilst filed. Only one-third of state hospitals carry out any kind of security audit on their files.[32] Other findings include the following[33]:

- 64% of public hospitals do not comply with said law, not including hospitals in Madrid, Cataluña, and País Vasco (these are autonomous regions and have their own processes for handling information security, and hence did not participate in the survey). Only 15% of private medical establishments are not in compliance;
- Nearly 40% of public hospitals do not have a log of who accessed health information, compared to 15% of private hospitals;
- 30% do not have a method to prevent loss of data while being transported;
- 35% do not have a method to prevent access to health information (ibid);
- Public hospitals cannot be fined since it would essentially be a tax on the Spanish public, and not a penalty on hospital managers. Private establishments can be fined, no problems there;
- Only 92% responded to the survey. Twenty private hospitals are facing fines between 60,000 and 300,000 euros for not responding. Twenty-three public hospitals will have the incident go on their records;
- 202 hospitals that were singled out will have 6 months to rectify their shortcomings. Among these, private institutions

[26] Jowitt, Tom, (2010). NHS Tops ICO List For Most Data Breaches. eWeek Europe. Available at: http://www.eweekeurope.co.uk/news/nhs-tops-ico-list-for-most-data-breaches-7429.

[27] Doyle, E., (June 15, 2011). NHS Researchers Lose Laptop With 8 m Patient Record. eWeek. Available at: http://www.eweekeurope.co.uk/news/nhs-researchers-lose-laptop-with-8m-patients-records-31810.

[28] Asperger's charity loses children's data in laptop theft (2011). BBC. Available at: http://www.bbc.co.uk/news/uk-england-south-yorkshire-13574389.

[29] Laja Sade, (2011). Yorkshire trusts admit data breaches. Guardian. Available at: http://www.guardian.co.uk/healthcare-network/2011/jan/11/yorkshire-trusts-admit-data-breaches.

[30] http://www.security.nl/artikel/29712/1/Ongeanonimiseerde_112-meldingen_op_Internet_gelekt.html.

[31] http://www.security.nl/artikel/33800/1/CBP%253A_Jusititie_faalde_in_beveiliging_pati%25C3%25ABntenkaarten.html.

[32] http://www.databreaches.net/?p%3D14664; http://www.publico.es/espana/341421/el-60-de-los-hospitales-publicos-no-protege-los-datos.

[33] http://www.alertboot.com/blog/blogs/endpoint_security/archive/2010/10/14/medical-data-security-spain-has-problems-too.aspx; http://www.databreaches.net/?p=14664; http://www.publico.es/espana/341421/el-60-de-los-hospitales-publicos-no-protege-los-datos; http://www.abc.es/20101014/sociedad/hospitales-datos-201010140430.html; http://www.elmundo.es/elmundo/2010/10/13/espana/1286968504.html; http://www.cope.es/sociedad/13-10-10–uno-de-cada-tres-hospitales-espanoles-no-respeta-la-ley-de-proteccion-de-datos-220892-1.

face penalties between 300,000 and 600,000 euros for non-compliance;
- More than 90% of hospitals follow the proper disposal methods for medical documents;
- The law requires biannual audits regarding information security;
- 20% of Spanish state hospitals do not have ways to audit security incidences; 66% do not conduct audits at all. 88% of private establishments do conduct these audits.

Widespread risks and failures such as those illustrated above, particularly when they entail the misuse or breaches of personal data exposing the health of individuals, are likely to endanger user trust in the information society, more so now since data breaches occurrence are becoming more difficult to prevent and track.

The data on the medical information breaches indicate that the source of the threats come from the organisation through their internal agents who access data without authorisation for economic or non-economic motivates, from the organisation's lack of privacy and security policy and implementation, through accidental disclosure and from insiders who are legally privileged to access the information. Rostad and Edsburg (2006) for example report that 99% of doctors were given overriding privileges while only 52% required overriding rights. They also found that security mechanisms of health information systems were overridden to access 54% of patient's records. The problem is that such policy breeds potential misuse.[34] It is important to set up well-defined views that will allow personnel to access only a portion of a patient's medical records on a need-to-know basis. Identifying frequent threats across the health sector could help in developing effective information security.

5.2. *Data breach notification*

There is currently no general breach notification requirement in Directive 95/46/EC on data protection (Data Protection Directive). The European Commission in its ongoing review of the European data protection framework has indicated its intention to introduce a general data breach notification obligation and extend the scope of the breach notification regime to include all data controllers.[35] A number of countries, including Austria, Germany and Norway, have pushed ahead of the EC legislative agenda and have introduced national laws that include a notification requirement for data breaches. Member states had to implement the amendments to Directive 2002/58/EC on the protection of privacy in the electronic communications sector (Privacy and Electronic Communications Directive) last May 25, which introduced a breach notification requirement for providers of publicly available communication services, such as internet service providers and telecommunication operators.

The amended Privacy Directive defines "data breach'" to include any breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. The Article 29 Working Party had argued that it made no sense to restrict notification laws to telecoms firms when so many other companies hold citizens' personal data.

> "*An extension of personal data breach notifications to Information Society Services is necessary given the ever increasing role these services play in the daily lives of European citizens, and the increasing amounts of personal data processed by these services. Online transactions including access to ebanking services, private-sector* ***medical*** *records and online shopping are few examples of services that may be subject to personal data breaches causing significant risks to a large number of European citizens. Limiting the scope of these obligations to publicly available electronic communications services would only affect a very limited number of stakeholders and thus would significantly reduce the impact of personal data breach notifications as a means to protect individuals against risks such as identity theft, financial loss, loss of business or employment opportunities and physical harm*".[36]

In the EU, there are countries with statutory law and guidance on breach notification requirements across sectors (such as Germany). In other countries, neither specific rules nor guidance exist. Furthermore, it is much more difficult and expensive for plaintiffs and class action suits to bring civil cases concerning data breaches.

The revamp of the data protection legal framework in Europe should clarify the rules surrounding the use and processing of electronic patient records and breach notification.

5.3. *Different interpretation of the Data Protection Directive*

Despite the fact that Directives 95/46/EC and 2002/58/EC are uniformly applied in Europe, there are vast differences in the way certain elements of the Directive are interpreted and implanted by Member States' authorities and the courts. In some cases, transposition or practice has not been conducted in-line with the Directive. The existing framework lacks predictability. For instance, the EU Commission has argued that 40% of the UK's Data Protection Act is non-compliant with the provisions of the Directive.

Data protection authorities (DPAs) take varied approaches to enforcing data protection and privacy with some enforcing stricter rules and adding tighter requirements. For example, the Danish law states that the controller is liable for "any damage caused by the processing of data in violation of the provisions of this Act unless it is established that such damage could not have been averted through the diligence and care required in connection with the processing of data. In the

[34] Edsberg, O., and Røstad, (2006). study of access control requirements for healthcare systems based on audit trails from access logs. In: Proc. of the 2006 Annual Computer Security Applications Conference, Miami Beach.

[35] (A comprehensive approach on personal data protection in the European Union COM (2010) 609 final, 4 November 2010).

[36] Opinion 1/2009 on the proposals amending Directive 2002/58/EC on privacy and electronic communications (ePrivacy Directive). Available at: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp159_en.pdf.

Netherlands, the law says that the level of damages can be reduced depending on the extent to which the person being sued can be held accountable for the damage – but this latter matter is to be determined in accordance with the ordinary rules on full or partial liability."[37]

In Luxembourg, the Netherlands and Portugal, "genetic data are formally defined as data on health (Luxembourg, Netherlands) or on health and sex life (Portugal]) and thus brought within the category of sensitive data, while in Sweden the processing of such data is specially regulated, although they are not formally regarded as falling within the specific category to which the rules on "sensitive data" apply. The law in Luxembourg also defines "genetic data" as "information of inherited characteristics of an individual or a specific group of individuals".[38]

This illustrates the vast differences in the way the directive is interpreted. The current situation, where 27 Member States have to implement a Directive into their national law, leads to these diverging uneven and vague implementations and limited enforcements. Organisations operating in multiple jurisdictions face the difficulty of ensuring compliance with numerous interpretations.

The availability of telemedicine also creates serious regulatory challenges. Those challenges are complex where the provider and receiver are in the same country, and even more complex when the provider is not in the same country as the recipient. The entry into force of the Directive on the application of patients' rights in cross-border directive and the EU plan to have a centralised EHR system will result in increased exchange of information between healthcare providers in different Member States. These developments all point to the need to strengthen the safeguards for health information to prevent abuse and disclosure to unauthorized third parties.

5.4. *Data retention*

An important issue in EHR is the storage and preservation of health records especially since they are integrated and made accessible to different stakeholders such as primary care physicians, hospitals, insurance companies, and patients. Records have the potential to be created, used, edited, and viewed by multiple independent entities.

Although the Data Protection Directive prohibits the retention of personal data for longer than necessary, health providers can retain the records for longer than the periods when supported by explicit reasons. The required length of storage of an individual electronic health record will depend on national and state regulations, which are subject to change over time.

In the EU, there are rules in relation to records of clinical trials (20 years retention period), but there is no specific legislation on the maintenance, control and retention of medical records except for the Data Protection directive which sets out only general rules. Some hospitals store records indefinitely, while others destroy them after storing them in microfilm.

The separate statutory regulations governing the retention of medical data for scientific research that exist in certain other European countries are based on an exceptional provision within the Data Protection Directive. This states that Member States may, for reasons of important public interest, formulate (by statute or decree) additional derogations from the prohibition on the processing of sensitive personal data.

In Spain, the "Patients' Rights Law" governs healthcare and decision making. According to Article 17 of the Spanish Patient's Right Law, "Healthcare centres are obliged to preserve medical files in such a way as to guarantee their correct maintenance and safety, even those not necessarily in the original format, in order to be able to provide due assistance to the patient for a period of time adapted to each case and for a minimum of five years from the date of discharge of every period of care. Medical files are kept for legal purposes in accordance with current legislation." In general, the patient's record is kept throughout the patient's lifetime and 20 years after the death.[39] In Germany, reports are part of the patient's record and kept for 30 years.

In the Netherlands, the general retention period for medical files 15 years. There are some exceptions to the general 15-year retention period, namely in the case of:

- good care provider practices *or*
- statutory obligation *or*
- patient's request *or*
- anonymous details *or*
- the interest of others.

The medical data may be retained longer if this is a reasonable consequence of the care provided by a good care provider. A statutory retention period of 5 years after the end of the involuntary admission applies to the files of psychiatric patients who were admitted under a hospital order. For psychiatric patients who were admitted voluntarily the general retention period of 15 years applies. The Archiefwet [Public Records Act] applies to certain data in university hospitals. Documents such as the surgical procedure report and the discharge letter must be kept for 115 years. Data relating to a medical check-up must be kept as long as needed for the objective for which the check-up was performed. This will usually be less than 15 years.[40]

Unless the patient him/herself requests that the data be destroyed earlier, the care provider must keep them for as long as is necessary in order to be able to provide him or her with a proper standard of care, with the minimum period being ten years.[41]

[37] Douwe, Korff, (2002). EC Study on implementation of data protection Directive.
[38] Id.
[39] http://www.alzheimer-europe.org/DE/Policy-in-Practice2/Country-comparisons/Healthcare-and-decision-making-in-dementia/Spain; http://www.alzheimer-europe.org/DE/Policy-in-Practice2/Country-comparisons/Healthcare-and-decision-making-in-dementia/Spain; http://www.mir-online.org/html/img/pool/Laurence_Sutton.pdf.
[40] Handling of Your Medical Data (2009). Available at: http://www.dutchdpa.nl/Pages/en_inf_subj_Handling_Medical_Data.aspx.
[41] Health Council of the Netherlands. The term for retention of medical records. The Hague: Health Council of the Netherlands, 2004; publication no. 2004/08.

In the UK, the Data Protection Act provides guidance on record retention in terms of principle that the "data shall not be kept longer than is necessary". In the absence of a defined period in the Act, the code of practice provides suggested guidance to the NHS as to what a suitable minimum retention period of a health record should be, based on professional good practice (Table 1).

In Ireland, the contract between GPs and the Health Service Executive (HSE) includes a general requirement to keep "adequate clinical records" but does not set any standards about the type of medical records to be maintained or the length of time for which they should be retained. The HSE's Code of Practice for Healthcare Records Management 2007 Code sets out detailed standards for the creation, maintenance and storage of health records. These standards are meant to apply to all healthcare facilities. It sets out the recommended retention periods for health records in publicly funded hospitals. The appropriate retention period depends on the type of records involved. General healthcare records should be retained for 8 years after treatment ceases or after the patient's death. Children's records should broadly be retained until they reach the age of 25 or 26. Some records must be retained for up to 30 years (for example, records which may be required in criminal proceedings).[42]

Care providers and patient organizations are concerned that data are being lost that may subsequently once again prove to be of importance to the care of patients or their relatives. Researchers stress that exposure to a particular routine treatment may possibly, still after even ten years, prove to have late consequences that merit closer investigation. According to the Health Council of Netherlands:

> *Diseases that were previously fatal are now treatable, but this frequently means that people have to reckon with an increased, lifelong risk of relapse. A hereditary factor is being found to play a role in an increasing number of diseases and conditions. Members of the patient's family may also have an interest in the fact that his/her data are not destroyed after ten years. Furthermore, various correlations between previously experienced diseases or treatments and the possibility of health problems emerging later in life are more widely understood and taken into consideration. It is important – both for the research into these conditions and for the further care of patients who have been exposed to treatments that have been revealed to have late complications – that medical data should be retained for (much) longer than ten years. The meant research also requires that retention does not stop after the death of the patient.*

The lack of harmonised data retention period for medical data has made the compliance management process in European healthgrids very challenging. Medical data that are destroyed after the retention period in a Member State may prove vital in saving the life of the patient who has relocated in another state. On the other hand, a long retention period could also unnecessarily expose the person concerned to risks associated with the illegal access and transfer of his or her personal data.

Table 1 – UK medical record retention period.

Type	Retention period
Maternity records	25 years after the birth of the last child
GP records	GP Records retain for 10 years after death or after the patient has permanently left the country unless the patient remains in the European Union. In the case of a child if the illness or death could have potential relevance to adult conditions or have genetic implications for the family of the deceased, the advice of clinicians should be sought as to whether to retain the records for a longer period. Electronic patient records (EPRs) must not be destroyed, or deleted, for the foreseeable future.
Records relating to persons receiving treatment for a mental disorder within the meaning of mental health legislation	20 years after the date of the last contact; or 10 years after the patient's death if sooner
Records relating to those serving in HM Armed Forces	Not to be destroyed
Records relating to those serving a prison sentence	Not to be destroyed

Source: Department of Health (2006) Records management: NHS code of practice.

5.5. *Different levels of security*

The Data Protection Directive specifies that appropriate technical and organisational measures must be taken against unlawful or unauthorised processing of personal data and to protect personal data against accidental or unlawful loss, alteration, damage or destruction.

Although the strict protection of health data is a responsibility of all Member States, there is currently no commonly accepted definition of an 'appropriate' security level for healthcare within EU which could be applied in the case of cross-border healthcare. Different states have their own security requirements.

> *So, for example, a hospital in one Member State may be obliged by nationally imposed data protection regulations to adopt specific security measures (e.g. the definition of security policy and codes of conduct, specific rules for outsourcing and use of external contractors, auditing requirements, etc.) whereas in other Member States this might not be the case. This inconsistency may have impact on the cross-border data exchange, especially when in electronic form, since it cannot be guaranteed that data are secured (from a technical and organisational point of view) at the same level between different Member States. In this sense, the main area of consideration is the security of the*

[42] Patients' rights – Medical records and access to health services. The journal of developments in social services, policy and legislation in Ireland. July 2008 Volume 35: Issue 10.

processing, i.e. the measures (technical and organisational) that the Member States take to safeguard the security of health data.[43]

6. Conclusion

A centralised EHR allows access to health information anyplace and anytime. EHR can enhance effectiveness, reduce costs, accuracy, currency, completeness, accessibility and generally improve the quality of healthcare services. Healthcare entails complex delivery systems involving teams of doctors, nurses and others, and clinicians, regulators, auditors, and trainees who all need to access and use medical records. Nonetheless, it also leads to an increase in the amount of information that is collected, sorted, filtered, transferred or otherwise retained, and the risks to such data therefore multiply raising the potential abuse and the risk of violation of privacy. Furthermore, the diversity of health systems, especially with respect to quality and safety policies in Europe, is as a major stumbling block for enabling the deployment of cross-border EHR. Other problems which need to be addressed include the interoperability of databases containing individual's health information, acceptable standards, jurisdictional boundaries, confidentiality, semantic-based knowledge representation, security, breach notification and compliance with data protection and other legislation.

Evidence also suggests that major source of privacy threats are internal factors and not external.

Despite the benefits of widespread EHR adoption, its implementation and acceptance will not be achieved unless the risks to privacy and security are mitigated. It is therefore crucial that privacy and data protection are embedded within the entire life cycle of the EHR from the very early design stage to its ultimate disposal.

Patrick Kierkegaard (*Patrick.Kierkegaard@diku.dk*), *Department of Computer Science, University of Copenhagen, Denmark; International Association of IT Lawyers, Denmark.*

[43] Opinion of the European Data Protection Supervisor on the proposal for a directive of the European Parliament and of the Council on the application of patients' rights in cross-border healthcare. Text available at: http://eur-lex.europa.eu/Notice.do?mode=dbl&lang=en&ihmlang=en&lng1=en,en&lng2=bg,cs,da,de,el,en,es,et,fi,fr,hu,it,lt,lv,mt,nl,pl,pt,ro,sk,sl,sv,&val=496183:cs&page=.