ELECTRONIC HEALTH RECORD

BEUC POSITION

Contact: Ilaria Passarani–health@beuc.eu

Ref.: X/2011/059 - 19/07/11

BEUC, the European Consumers' Organisation
80 rue d'Arlon, 1040 Bruxelles - +32 2 743 15 90 - www.beuc.eu
🕮**EC register for interest representatives**: **identification number 9505781573-45** 🕮

Summary

Electronic health records (EHRs) are an important tool that could improve safety, quality and continuity of care. They could also help to make health care systems more efficient and more responsive to patients' needs. At the same time, the storage of sensitive health information in an electronic form opens a new risk scenario and poses many challenges that need to be addressed. In particular, it is important to:

- Guarantee that consumers' health data are fully secured and protected;
- Grant consumers easy access to and control over their electronic health record;
- Ask consumers their informed consent for the storage and sharing of their health data;
- Adopt a proper identification and authentication system for consumers and health care professionals;
- Put in place a system of data modules to find the right balance between accessibility and data protection;
- Reinforce the legal framework on data protection (e.g. privacy by default, multi-layered liability, etc);
- Promote interoperability;
- Secure the system from a technical point of view against breaches and crashes;
- Give consumers the tools to seek redress and compensation in case of breaches of privacy;
- Enforce dissuasive penalties against abuses.

For the electronic health records to be used and accepted it is necessary to:

- Inform consumers about the benefits and the shortcomings of the EHR;
- Make a benefit/risk and a cost/benefit analysis based on sound and independent evidence before further deploying EHR systems;
- Ensure the transparency of EHR systems in terms of content and functioning;
- Develop EHR systems with, for and around the patient;
- Educate consumers and train health care professionals.

1. The potential benefits for consumers

The Electronic Health Record (hereafter EHR), is defined 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. It can compile information on the past and present state of health of a person, and for a considerable period of time, maybe even a lifetime"[1]. EHRs can include information on patient treatment progress, medications, vital signs, past medical history, laboratory data and radiology reports.

There is still a lack of evidence on the overall implications of eHealth (see paragraph 9), but subject to a comprehensive analysis of the benefits and the risks, the EHR has a lot of potentials as it could be an important instrument to improve safety, quality and access to health care. The ageing of the population, the consequent higher number of people affected by chronic diseases, increased citizens' expectations for high quality health services, the shortage of health care providers and rising costs are challenging the sustainability of health care systems. In this context the possible benefits of EHR could be substantial in increasing efficiency, effectiveness and costs savings.

EHRs could help empower patients by providing them with easier access to their health information, allowing them to exert more control over their health records, thereby becoming more responsible and more active in their own care while facilitating communication with their healthcare professionals.

Furthermore, storing and transferring patient information electronically has the potential to significantly reduce clinical errors and improve patient safety, as well as allowing clinicians to communicate more quickly and accurately by identifying relevant information more easily. It could contribute to the avoidance of cases where, for example, the same exam is performed twice, a better understanding of the patient's medical history and also ensure continuity of care. From a patient's perspective this could mean a higher quality of care and more sustainable healthcare systems.

Finally, EHRs could be useful for health research purposes and for policy decisions: if managed appropriately and if the data can be fully pseudonymised (condition that at the moment cannot be fulfilled[2]) a huge amount of medical data could be easily collected and be used in various scientific studies, including epidemiological analysis, evaluation of health care procedures, pharmacovigilance etc.

[1] Article 29 Working Party Working Document 131 on the processing of personal data relating to health in electronic health records (EHR), 2007.
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp131_en.pdf
http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp131_en.pdf

[2] No Place to Hide — Reverse Identification of Patients from Published Maps, New England Journal of Medicines, 2006; 355:1741-174.http://www.nejm.org/doi/full/10.1056/NEJMc061891#t=article

2. A new risk scenario

The EHR opens a new risk scenario[1] for processing of personal health data, exposing consumers to the risk that their health information could accidentally end up in the hands of unauthorised parties. The unauthorised disclosure of a medical condition or diagnosis can negatively impact an individual's personal and professional life. The possibility of abuse is substantial and the risk increases when the systems become more interconnected. This means that consumers, healthcare professionals and decision-makers still have major concerns regarding the security of the system and are reluctant to use these new technologies.

In 2010 the consumer organisation Test-Achats conducted a survey among 930 consumers exploring the main concerns of consumers regarding the EHR. The results[3] which were published in November 2010 show that 56% of consumers believe that the use of internet to store their medical data is not safe, and does not guarantee the privacy of their data.

Health care professionals are also concerned about the privacy of patient data, and fear that the data in the system may be accessible to those who are not authorized to obtain them[4]. In the Netherlands, after investing almost a decade and several hundred million euro in developing the EHR, the implementation plan presented by the Ministry of health was rejected by the Parliament due to privacy concerns[5].

The European Data Protection Working Party is of the opinion that all data belonging to the patient in EHRs should be considered as "sensitive personal data". This qualification has implications for the level of security that is necessary to guarantee the safety of the data.

The EHR can create a route of access to medical data, for health care professionals, the patient themselves, and approved third parties via the internet. This poses significant challenges in ensuring that only authorised health professionals gain access to information for legitimate purposes related to the treatment of the patient[6]. Thus for EHR to be trusted and accepted, it is essential to guarantee that consumers' health information is fully secured and that all sensitive data are protected[7].

Provided that health data in paper form are usually considered not widely accessible, maintaining the legal standard of confidentiality suitable within a traditional paper form may be insufficient to protect the privacy interests of a patient in the new situation. Therefore, the deployment of EHR systems should be preceded by the reinforcement of the legal framework on data protection, including the introduction of a legal definition of "multi-layered liability' and of 'health data".

It is also important to encourage the deployment of security-enhancing technologies and services to prevent and fight identity theft and other privacy-intrusive attacks. Privacy by design and by default should be embedded in the development of the technology systems of EHRs with the highest level of privacy and security. Guidelines must be provided on notification processes should a breach occur. This should be addressed in the context of the revision of the Data Protection Directive.

[3] Test-Sante, n.99, November 2010.

[4] Boonstra, A. Broekhuis, M (2010). Barriers to acceptance of EMR by physicians. BMC Heath Services Research 10:231.

[5] News article retrieved from www.anp.nl on 5 April 2010.

[6] Test-Saude, n.84 April, 2010.

[7] Tensions and Paradoxes in Electronic Patient Record Research: A Systematic Literature Review Using the Meta-narrative Method. Greenhalgh, T. Potts, H. Wong, G. Bark, P. Swinglehurts, D. University College London. The Milbank Quarterly, Vol. 87, No. 4, 2009 (pp. 729–788).

When allowing the use of compiled and anonymised data from EHRs for research purposes it is necessary to take into account that technological advances in data analysis and the combination with other data set could endanger anonymity and lead to the identification of individuals.

Unless strict rules exist regarding the security and accessibility of health data, the risk of use by third parties, such as insurance companies, cannot be excluded. A recent study about the security of medical records in Dutch hospitals showed that almost 75% of all hospitals do not comply with the current national code of information security[8]. Before the implementation of the EHR goes any further, these privacy concerns must be addressed.

Moreover, the use of sensitive health data for marketing purposes should remain prohibited.

Finally, EHR systems should be fully safe from a technical point of view and have backup system in case of catastrophic system crashes.

3. Consumer access and control

The EHR is about consumer's health and it should be in "his/her hands". Consumers have the right to be in control of the use that is being made of their data and should be able to access their record anywhere and anytime. Due to new models of care and more specialisation, patients' information will be more and more shared between many health professionals and consumers should have assurance that what is indicated both about themselves (e.g. contact details) and their medical condition is correct[9]. The patient is the one most concerned about the accuracy of the information and he/she the one who can verify that the information is fully correct. The option to access one's own information is a fundamental right that is embodied in the European Union Data Protection legislation[10]. To ensure that consumers have complete control over their own medical files they should have the option not only to view their record, but also to add information under certain specific conditions - for example in a dedicated session, with a limited amount of characters available and without directly amending the EHR or deleting parts - in order not to raise liability issues. Health care professionals should take into account the consumers annotations and if relevant modify the content of the EHR accordingly[11] and timely. The owner of the health record should be informed every time a health care professional who is not the one who is directly treating him demands access to his or her file, and should be asked to give the authorisation to access to the whole file, or parts of the file, or no access at all before the information is accessed. According to the survey made by Test-Achat (see above) 95% of the consumers interviewed expressed the desire to view their own medical files. 89% of them believe that it is important to see who accessed their medical file and 74% said they want to be asked for the authorization before their record is shared with other health care professionals.

[8] Niscayah 2010.VoortgangsrapportageElectronischPatienten Dossier. Retrieved from http://www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2009/11/11/voortgangsrapportage-elektronisch-patientendossier.html

[9] Position Paper on eHealth: The Electronic Patient Record. European Health Telematics Association (EHTEL). 25-09-2006.

10Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and Directive2002/58/EC on privacy and electronic communications.

[11] Mandl,K.,Szolovits, P.,Kohane, I.S. (2001) Public standards and patients control. BMJ;322;283.

Due to the fact that nobody can be forced to take part in an EHR system the question of possible complete withdrawal from an EHR system ought to be addressed as well. This withdrawal from the EHR system should be well informed and should not affect the medical treatment of the consumer. If patients refusing the EHR suffer disadvantage (e.g. substantial additional costs) consent cannot be considered sufficiently free[12].
Reliable identification of patients in EHR systems is of crucial importance to ensure the right treatment and to prevent medical mistakes, but it is also important to identify the person logging in to his or her personal data. The Data Protection Working Party recommends that health cards on smart card basis could contribute significantly to a proper electronic identification of patients and also to their authentication if they want to access their own EHR data[1].

To ensure that the EHR is accessible and understandable for all consumers, the layout of the EHR should be easy to understand and reader friendly. Technology associated with EHR could be difficult to use, because of lack of internet access or understanding of computer systems[13]. In the Netherlands for example, according to the Citizen's Service Number Act, health care providers must provide a "client counter" for file consultation. At the counter consumers can not only access their file but also indicate to which (groups of) health care organizations information might be provided or the permission withdrawn. How this counter can operate in practice still needs to be assessed.

4. Health care professional access

Consumers should be reassured that only authorised and specifically trained health care professionals have access to their EHR. Specific identification and authentication systems should be put in place to verify the identity of the patient and of the health care professional and to ensure that data are only accessed by people who are directly involved in the patient's treatment, and have permission to access the data.

In the Netherlands, health care professionals could access medical data stored with other health care providers via a Unique Healthcare provider identification register (UZI). This system was implemented in 2006, however it was hacked in 2010. All the UZI cards had to be retrieved and new cards with different chips were made. Widespread EHR systems cannot be put in place until it is guaranteed that these situations cannot occur.

Access to patients' health records should only be permitted to the health professionals directly involved with the patients' condition.
Different modules with different levels of security should be implemented. With a system of data modules or sealed envelopes certain professionals could be granted access to the whole file while others only to certain parts of the file. For example genetic or psychiatric information could be sealed in an envelope accessible only to few health care professionals and only with the prior and explicit consent of the patient while emergency information could be contained in a separate module more widely accessible in case of need (e.g. when the patient is unconscious).

[12] Opinion 15/2011 of the Article 29 Data Protection Working Party, 13 July 2011.
[13] Report on Health IT Systems. The Danish Consumer Council. Forbrugerradet, May 2010.

EHR makes it easier to make copies of the file and this poses a series of risks. When a consumer requests to remove certain things from his/her file the consumer will have to search for all the copies that have been made and ask for the deletion[14]. This is a complicated and time consuming process, and cannot be expected from consumers. To control this there should be an easy way to gain knowledge about every time a file is requested, by whom, and for which reason. There must be a tracking system of every access to the health records.

5. Informed consent

Consumers have the right to know what data is collected and stored, how this data is accessed and processed and by whom, for how long data is retained and for what purpose, as well as what their rights are in case of breaches.

Only when they are fully informed, they can make an accurate decision and provide their clear, free and explicit consent about the processing of their health data. This informed consent should be the basis of all actions with regards to consumer's medical data, whether it is exchange, analysis, adaptation or deletion of medical data.

In order to be valid consent must be freely given, unambiguous, specific, explicit and informed[10]. Exceptions should be considered in case of emergency care.

Despite it is possible that such a consent may not be required when health data are processed by a health professional for reasons related to preventive medicines, medical diagnosis, the provision of case or treatment or the management of health-care services[15], the fact that the data included in the EHRs may be accessible to a variety of entities renders it important to clarify the application of the rules on consent and ensure the security of the data.

6. Supervision and enforcement

Consumers have the right to know when break-in, theft or loss of personal data occur. Incorrect use like when unauthorized persons/entities get access to the records or use them for purposes other than the ones they have been collected for should also be considered as misuse. In case of a breach of security, leading to the accidental loss, alteration, or unauthorised disclosure of personal health data, the individuals concerned and the national data protection supervisory authorities should be promptly informed. In these situations consumers should have legal grounds to file a complaint and seek compensation, including via collective redress mechanisms if a high number of people suffer damages. Dissuasive penalties should be enforced to prevent abuses.

Another issue of concern is the question of liability. With the EHR, due to the wide range of users who have access to the same medical file, it is difficult to establish where mistakes are made. It is therefore necessary to establish multi-layered liability for the entities involved in the processing of data included in the EHR.

[14] Position Paper on the Electronic Patient Record.Consumentenbond, 2007.

[15] European Union Data Protection Directive 95/46/EC.

7. Education of consumers and training of health care professionals

In order to gain their trust in the system, consumers must be educated about the content and the functioning of the EHR systems and should be questioned regarding the level of satisfaction with the service. In this respect, knowledge needs to be gained on how to influence cognitive, physical, or literacy barriers on workflow and outcomes of using health records. EHRs should be user-friendly and be designed with the involvement of consumers. Consumers should have also alternative conventional means to access personal health data. In this context it is important to ensure that the information uses language and a layout that is easy to understand also to people with special needs (e.g. elderly).

With the growing introduction of ICT services in all phases of the care process, the physician's responsibilities also increase. Therefore there is a need to train health care professionals to make adequate use of this these technological innovations, without affecting the doctor-patient relationship[16].

When speaking about EHR it is worth noting that access to the internet is not universal. A study[17] from the European Commission in 2007 shows that only 60% of all general practitioners use a computer during a consultation (EU27). The national percentages vary form 100% in Finland to only 8% in Italy. The communication and exchange of data between hospital and general practitioner within Europe only happens in 20% of all cases (EU27). These national data vary from 76% in Denmark to 0% in Romania. These data show that there is still a long way to go before the use of EHRs become a reality in medical practice and that digital literacy has to be addressed in order not to increase inequalities.

8. Interoperability

Interoperability of EHR systems means the transfer of personal data regarding the health of an individual. In principle information about a patient should flow freely between the various health care professionals directly involved in the patient's care, between different health care settings, provided that the patient gives his/her consent. Interoperability between the different operating systems is crucial in ensuring the effective implementation of the EHR and the successful deployment of eHealth at national and at European level. EHRs that are readable by clinicians in different settings and languages could enable safer treatments, avoid duplications and reduce costs.

Whereas, at national level it might be easier to ensure the interoperability between all EHR and the access through a central database, this is not granted at EU level. Interoperability of EHR was defined as one of the main priorities for Member States in the Roadmap of the Community eHealth action plan in 2004 and has been reaffirmed as a key issue in the Council Conclusions on Safe and efficient healthcare through eHealth in 2009 as well as in the Directive on the application of patients' rights in cross border health care in 2011 but it is far from becoming a reality.

[16] Boonstra, B. Broekhuis, M. (2010) Barriers to the acceptance of electronic medical records by physicians from systematic review to taxonomy and interventions. BMC Health services Research 10:231.

[17] http://ec.europa.eu/information_society/eeurope/i2010/docs/benchmarking/gp_survey_final_report.pf

We believe that at the moment it is hindered mainly because of legal and technical issues but also by cultural barriers. An adequate legal framework and networked infrastructures should be built to cover the entire continuum of care. A change of culture in the health care management system and in the health care professionals' approach is also needed: the system should not be designed around the physician, the hospital or the insurance system but should be designed for and around the patient. All the measures should be put in place to allow the EHR to move together with the patient, including when seeking health care in a Member State different from his/her own country[18].

The interoperability of EHR at European level brings several challenges to the development of the EHRs themselves. Interoperable systems do not only have to overcome language barriers but also differences in countries' healthcare systems and differences in the implementation of the data protection legislation. In addition the use of different and often conflicting technologies and standards may render the interconnection of databases and EHRs impracticable. In this context it is important to introduce a new right to data portability i.e. the right to recover and/or to shift data posted from one platform/cloud to another. It implies that consumers should retain ownership over their data online at all times.

Incompatibility and lack of interoperability between different databases and systems can be reduced with the adoption of consistent technology and standard data, whilst effective cooperation between general practitioners and patients to record historical data could also be improved. The European Commission Recommendation on cross border interoperability[19] claims that "semantic interoperability" is an essential factor in achieving the benefits of EHR to improve quality and the safety of patient care. Wherever possible, Member States should consider the suitability of international medical-clinical terminologies, nomenclature and classifications of diseases. This should aid the comprehensiveness of the EHR throughout Europe. Interoperability of EHR should also be implemented on a technical level and for this purpose it is advisable to undertake a survey of the existing technical standards and infrastructures that may facilitate the implementation of EHR systems and their interoperability.

9. More research on the benefits, the costs and the risks associated with EHRs

The scientific evidence regarding the benefits of EHR on quality of care and on the health care budgets is conflicting. In 2009 the European Commission published a report on the socio-economic impact of interoperable EHR and ePrescribing systems in Europe[20]. For all cases analysed, the socio-economic gains to society from interoperable EHR and ePrescribing systems eventually exceed the respective costs. One of the key finding of the study is also that the benefits from EHR and ePrescribing investments come under some broad, diverse categories, that their instantiation is very specific to the context and that the benefits can be measured only after a considerable period of time.

[18] BEUC Position on Cross Border Health Care, 2008.

[19] Commission Recommendation on cross-border interoperability of electronic health record systems July 2008.

[20] The socio-economic impact of interoperable electronic health record (EHR) and ePrescribing systems in Europe and beyond - Final study report, European Commission, October 2009.

At the same time a systematic literature review[21] of studies on the impact of e-health on the quality and safety of care concludes that "There is a large gap between the postulated and empirically demonstrated benefits of eHealth technologies". In addition, there is a lack of robust research on the risks of implementing these technologies and their cost-effectiveness has yet to be demonstrated, despite being frequently promoted by policymakers and "techno-enthusiasts" as if this was a given. In the light of the paucity of evidence in relation to improvements in patient outcomes, as well as the lack of evidence on their cost-effectiveness, it is vital that future eHealth technologies are evaluated against a comprehensive set of measures, ideally throughout all stages of the technology's life cycle. Such evaluation should be characterized by careful attention to socio-technical factors to maximize the likelihood of successful implementation and adoption.

Therefore, before investing in the large scale deployment of EHRs it is advisable to conduct additional research on the benefits, the costs and on the risks for privacy associated with their use. Public health benefits (e.g. quality of care, sustainability of the health care systems) should be weighted against individual risks (e.g. loss of a job because of breaches of privacy).

10. Conclusions

For EHR to bring benefits to consumers it is necessary to address some outstanding issues, namely data protection, consumer access, legal certainty and interoperability. Moreover, before investing in any large deployment of EHRs, a detailed cost/benefit and benefit/risk analysis is required. Only if and when these conditions will be met, and if the net benefit is found, it will be possible to exploit the full potential offered by this ICT solution and use it as a tool to make health care systems more efficient and more effective. In addition, for EHRs to be accepted by the consumer, the ultimate beneficiary of this technology, a change of culture in the healthcare management system and among healthcare professionals' is needed: EHR systems should not be designed around the physician, the hospital or the insurance system, but rather for the patient.

Finally it is important to take into account that in the health sector the technology cannot just simply be imposed and that it is necessary to involve the end users, health care professionals and patients, all along the process taking into account the human relationships that make the technology work.

END

[21] Black, A. Car, J. Pagliari, C et al. (2011) The impact of eHealth on the Quality and Safety of Health Care : a systematic overview. PLoS Med 8(1):e1000387. doi:10.1371/journal.pmed.1000387.