How Will the General Data Protection Regulation Affect Healthcare?

Como é que o Regulamento Geral da Proteção de Dados Irá Afetar a Saúde?

Nathan C. LEA✉[1]

Acta Med Port 2018 Jul-Aug;31(7-8):363-365 ▪ https://doi.org/10.20344/amp.10881

Keywords: Confidentiality; Delivery of Health Care; Electronic Health Records; Health Records, Personal

Palavras-chave: Confidencialidade; Prestação de Cuidados de Saúde; Registos Eletrónicos de Saúde; Registos de Saúde Pessoal

On 25th May 2018 a new European Union Regulation came into force. The General Data Protection Regulation (GDPR) has received a great deal of attention from citizens, governments, regulators and industry both across Europe and internationally.[1]

What is GDPR and what is its scope?

GDPR[2] is a Regulation that covers the protection of personal data – that being any data that identifies an individual. This could include anything from names and addresses to IP Addresses. GDPR also defines special categories of personal data, including health records, genetic data, biometrics, political opinions, trade union memberships, ethnicity and sexuality amongst others where additional provisions must be satisfied to handle it.

GDPR applies to all industries, including health, across the EU. It applies to all European Union (EU) citizens and any organisation handling their personal data regardless of where they may be in the world – it is extraterritorial in scope.

The older Data Protection Directive from 1995, which GDPR replaces, was a Directive where Member States had to implement laws that met its goals. As a Regulation, GDPR has to be applied directly in Member State Law, but there are various 'derogations' (or relaxations) of the law where Member States can adapt it to how their local laws, public services including health and so forth work.

This means that GDPR will need to be implemented by Member States by drafting their own laws for data protection. These implementing laws must also achieve the requirements of GDPR's Law Enforcement Directive, so will have specific provision for law enforcement in addition to the derogations. The new Portuguese Data Protection Act has not been enacted in law at time of writing.

Why is GDPR important?

The evolution of digital technology prompted the EU to recognise that the 1995 Data Protection Directive was out of date and needed modernisation to protect EU citizens.[3] Member States today rely on data driven co-operation and high capacity digital technology that were inconceivable in the 1990s. How useful are WhatsApp and social networking tools for medicine nowadays and how secure are they?[4,5]

Data scandals show the need for clearer laws on data protection. The use of data collected on Facebook by Cambridge Analytica is a clear example.[6] The Wannacry cyber-attack early in 2017 which crippled multiple sectors including health was a terrible wake-up call about data and technology vulnerability.[7]

Culture change – what does this mean for medical practice?

Industries like health that rely on safe handling of personal data and benefit from advances in technology need a catalyst for culture change and clarity on how to achieve it. GDPR can be that catalyst: it enshrines principles around the need for data processing to be lawful, for specific and clear purposes, accurate, available and sufficient to complete the tasks, securely handled and not excessive to achieve the purposes. It demands transparency and accountability, makes organisations think about protecting personal data in their risk assessments and allows for fines of up to €20 million or 4% of global turnover for serious breaches of the law.

If anything, GDPR makes us all think more carefully about how we handle and protect data. It prompted the health and research communities to mobilise across Europe since 2012 to ensure that practice of health and research would not be compromised by a prohibitive drafting of GDPR[8,9] so health is very much a part of its fabric.

Implications for health organisations

The onus of GDPR's impact is likely to be for health organisations, hospitals, general practice surgeries and other healthcare organisations because they act as both a data controller (responsible for deciding why and how data is processed) and as processors when handling data. This means they have to support staff who carry out these roles on a day to day basis.

GDPR requires accountability for how people and

1. University College London. London. United Kingdom.

✉ Autor correspondente: Nathan C. Lea. n.lea@ucl.ac.uk

Recebido: 01 de junho de 2018 - Aceite: 12 de junho de 2018 | Copyright © Ordem dos Médicos 2018

organisations handling personal data protect it, and this includes specifying what is allowed in contract, particularly when a health organisation hires a third-party company to handle data processing tasks. Responsibility for compliance is not just on data controllers, but also processors to ensure that their work and direction from controllers does not breach GDPR in any way.

Controllers and processors must be transparent about the processing of people's (or 'data subjects' – including patients and staff) personal data. They have to very clearly articulate how they are processing data in accessible notices, for clearly defined purposes and under clear legal bases, specifying people's rights and who they should contact to exercise them.

GDPR mandates the appointment of a Data Protection Officer (DPO) for public authorities like health providers, who uphold GDPR compliance. The DPO will liaise with data subjects when they wish to exercise their rights. They will also liaise with the Portuguese data protection regulator Comissão Nacional de Protecção de Dados (CNPD)[10] for example where there may have been a serious data breach, which GDPR requires is reported within 72 hours of discovery (and this is not restricted to working hours).

In brief, health organisations will need to be more transparent and rigorous in documenting their data processing activities, develop codes of practice and policy (for example when a breach occurs) and will need its staff to act carefully whilst making sure they have what they need to keep the data flowing securely for their reasonable purposes.

Clarifying consent

GDPR offers legal bases for processing data that do not diminish or undermine other legal principles around ethics or duties of confidence. It is therefore important to understand the role of consent in terms of treatment and data processing and how this may be clarified as GDPR is adopted. This also illustrates some of the points around special category data.

Where health and mental health data are concerned (amongst others), GDPR identifies these as a special category of personal data and stipulates additional provisions for their processing as defined under Article 9 of GDPR. These additional provisions include the need to process data to provide health care, run health care services and perform research amongst others.

Whilst consent is a legal basis for data processing under GDPR and also one of its additional provisions for processing special category personal data, it may not be the one for processing health data for the purposes of providing care. For this we look to Recital 43 of GDPR.[2] The legal basis for processing health data is more likely to be as a public task, in exercising the duties of a public authority in the public interest (in this case a health care provider providing care). The additional provisions under Article 9 are met due to the need to process data to provide care and run a health service in the interests of the public.

Patients must of course consent to treatment that requires practitioners and health service providers to treat them under a duty of confidence – that does not change. This consent would arguably not meet GDPR requirements for consent to data processing because for data processing GDPR directs that consent must be freely given. GDPR's consent requirements are that consent for data processing must be clear, for specific purposes, unambiguous, uncoerced, freely given and people need to be able to withdraw it as easily as they give it.

If patients are consenting to care that needs data to be processed, they have no apparent choice about whether it is processed and therefore cannot freely consent to the processing itself. They would also likely have difficulties in withdrawing consent for its processing as their care, and their treating physician, rely on it. They should however be aware of the processing need when they give consent for treatment pursuant to the consent requirements for treatment which GDPR does not change.

Where health data is used for other purposes like research, this again will likely need to be based on consent to participate as required by ethical practice and honouring the duty of confidence, but GDPR permits the data processing as part of a public task and the additional provision could be the necessity to process data to conduct research. These are the likely legal bases and additional provisions for special category data provided the research and data processing is in compliance with other Portuguese (or any Member State) laws.

In all cases, organisations must be transparent about the processing of the data for any purpose, including under any legal obligation. They should also be clear on the other legal bases available to them within GDPR and their Member State derogations when deciding the legal basis for processing.

Implications for 'data subjects' - patients and staff

GDPR enshrines rights for data subjects, some of which are new or significantly strengthened: the right for data subjects to ask for their personal data to be deleted, the right for them to be given a copy of it for their own uses, and their right to object to automated processing for example in profiling or where decisions are made through artificial intelligence. People can now ask for decisions made by computer to be overturned and ask for a human to control them and make them instead.

The other rights around access to personal data, objection to its processing, correction when it is wrong and restriction on its use are not necessarily new, but much more clearly defined. Data controllers now cannot charge people for accessing their data unless their requests become excessive.

But these rights are not absolute: data subjects cannot request data erasure that would cause them or the data controller or processor harm or need excessive effort to achieve. Patients cannot ask for whole sections of their medical record to be erased or deleted completely because

it would compromise their care, and their practitioner may rely on the record for their own needs, be that as reference or for their defence.

Implications for health care professionals

There are two important things to remember for GDPR: firstly, be very clear on what personal data you are handling, why you need to and its security; secondly, be prepared for more and clearer codes of practice when handling data and do any training that your health organisation or professional bodies ask you to do.

It is likely that you will be handling the vast majority personal data on a day to day basis. GDPR mandates codes of practice and competence in handling data, but the DPOs can help with understanding this. You should always refer to your organisations' guidelines, professional codes of conduct and those of CNPD.

But most importantly, remember that if you are in any doubt, ask your DPO or data protection champion. Where GDPR is concerned, it is always better to seek clarification than beg forgiveness. GDPR can be very beneficial to health care but will only succeed if we understand the need to handle data, protect it and further demonstrate trustworthiness to patients, colleagues and the wider public by honouring the newer legal requirements around meaningful transparency.

Where can I learn and read more about GDPR (in an easy to understand way)?

GDPR is a new law that has only just started to be enforced so guidance and support sources will be updated and become more available in the coming year or so. For a general guide, EUGDPR.org provides generic educational advice.[11] CPND[10] will likely update their pages particularly when the Portuguese Data Protection Act comes into force. You will also be able to find courses that offer awareness raising about GDPR and you should look at any recommendations that your professional bodies have around this. The European Patients Forum has also issued a guide for patients and patients' organisations that summarises GDPR from the patient perspective.[12]

DISCLAIMER

The article above reflects the author's opinions only and is for awareness raising but should not be taken as legal advice. In all cases, readers should consult their DPO or legal counsel for authoritative legal advice where necessary.

There are no competing interests to declare.

REFERENCES

1. European Commission. Commission publishes guidance on upcoming new data protection rules 2018. [cited 2018 May 31]. Available from: http://europa.eu/rapid/press-release_IP-18-386_en.htm.
2. European Parliament. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). Brussels: EP; 2016.
3. European Data Protection Supervisor. The History of the General Data Protection Regulation 2018. [cited 2018 May 30]. Available from: https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en.
4. Chan WS, Leung AY. Use of social network sites for communication among health professionals: systematic review. J Med Internet Res. 2018;20:e117.
5. Mars M, Scott RE. WhatsApp in clinical practice: a literature review. Stud Health Technol Inform. 2016;231:82-90.
6. Cambridge Analytica controversy must spur researchers to update data ethics. Nature. 2018;555:559-60.
7. United Kingdom National Audit Office. Investigation: WannaCry cyber attack and the NHS. 2017. [cited 2018 May 30]. Available from: https://www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs/.
8. The Academy of Medical Sciences. Positive outcome for research from EU data laws. 2015 23rd December 2015. [cited 2018 May 30]. Available from: https://acmedsci.ac.uk/more/news/positive-outcome-for-research-from-eu-data-laws.
9. Wellcome Trust. Data Protection Regulation 2018 [cited 2018 May 31]. Available from: https://wellcome.ac.uk/what-we-do/our-work/our-policy-work-data-protection-regulation.
10. Comissão Nacional de Protecção de Dados. Website for Comissão Nacional de Protecção de Dados Portugal 2018. [cited 2018 May 30]. Available from: https://www.cnpd.pt.
11. EUGDPR.org. EUGDPR.org 2018. [cited 2018 Jun 07]. Available from: https://www.eugdpr.org/eugdpr.org-1.html.
12. The European Patients Forum. The new EU Regulation on the protection of personal data: what does it mean for patients? [cited 2018 Jun 07]. Available from: http://www.eu-patient.eu/globalassets/policy/data-protection/data-protection-guide-for-patients-organisations.pdf.