Irish Journal of Medical Science (1971 -) (2019) 188:721–724
https://doi.org/10.1007/s11845-018-1857-3

LETTER TO THE EDITOR

General Data Protection Regulation (GDPR) and paediatric medical practice in Ireland: a personal reflection

Roy K. Philip [1]

Received: 26 May 2018 / Accepted: 21 June 2018 / Published online: 29 June 2018

Dear Editor

It appears that as my paediatric clinical practice is contracting the regulation around is steadily expanding and the 'new kid on the block' is General Data Protection Regulation (GDPR). While awaiting clear advice from regulators, professional bodies and health service executive (HSE), how should medical practitioners achieve an early GDPR compliance?

The confidentiality of patient records forms part of the Hippocratic Oath, and is central to the ethical tradition of medical practice. This tradition of confidentiality is in line with the requirements of Data Protection Acts of 1988 and 2003, under which personal data must be obtained for a specified purpose only, and must not be disclosed to any third party except in a manner compatible with that purpose [1]. As per the above acts, the Data Commissioner's view is that the patient's consent for the storage and use of their personal data is implicit in the fact that they come to a medical professional for help. However, it is good practice to inform patients that a practitioner will keep their details, and also to inform what use will be made of their data. Section 2(b)(vii) of the Acts allows for the processing of sensitive data for medical purposes by health professionals [1]. If patient details are urgently needed to prevent injury or other damage to the health of a person, then the details may be disclosed and section 8(d) of the Act makes special provision for such disclosures [1]. However, in non-urgent circumstances consent is needed in advance. Given the immense sensitivity of health-related information, it is imperative that healthcare professionals (HCPs) in this sector be clear about their use of patient's personal data.

GDPR came into European law on 25th May 2018 (Regulation 2016/679/EU) for the storage and processing of personal data in the EU. In addition, Data Protection legislation will be further enhanced by the Data Protection Bill of 2018 that will be signed into Irish law soon. GDPR has four major focus points: accountability, transparency, protection and reliability [2]. GDPR brings an onus to collect personal data for specific purpose only, to uphold the trust of the person who gives us their personal data, to maintain and protect the information and to erase it when no longer required [2]. A new heightened level of security, accountability, transparency and governance is required from the medical practitioner. Personal data (PD) and the special category personal data (SCPD) should be protected and EU is safeguarding the economic value of digitally kept information of citizens through GDPR [3]. In the wrong hands an amalgamation of multiple data points from the same individual potentially leads to identity frauds [3].

Although GDPR applies to all domains of the public and private sectors, some specific derogations are defined for data concerning health aiming at protecting the rights of data subjects and their confidentiality, whilst preserving the benefits of processing data for research and public health purposes [4]. Specific new obligations which healthcare providers should prepare include data access for patients and rules for data processing including explicit consent of the data subject [4]. Certain derogations and exceptions exist for healthcare and research. As per the Irish data commission website "organisations that only process manual data (unless prescribed by the Commissioner as requiring registration) is exempt" (full list in section 3 of SI657 of 2007). Even though majority of the information collected from patients are still in the manual format, in our current medical practice, there will always be some data that evade the above exemption clause and thus coming under GDPR [1–4].

Three components of professional activities coming under GDPR for Irish hospital consultants in clinical disciplines are (1) hospital practice within HSE, (2) private medical practice and (3) clinical research/clinical audits. Medico-legal professional roles warrant additional governance systems.

✉ Roy K. Philip
roy.philip@hse.ie

[1] Neonatology, Graduate Entry Medical School (GEMS), University of Limerick & University Maternity Hospital Limerick, LimerickV94 C566, Ireland

Hospital practice within HSE: Familiarise with and follow HSE's GDPR guidelines fully [5]. Data protection policies and processes have been in place in the HSE for many years. Key changes are the mandatory reporting of data breaches required within 72 hours and the requirement to respond to access requests to medical or other records within 1 month (previously 40 days) [5]. As per the GDPR website of HSE there is a recommendation to obtain consent from service users in areas such as clinical procedures (same as before). However, consent is not required to process the data of patients and service users [Article 6(1) and Article 9(2) of the GDPR] [1, 2, 5]. HSE staff members are expected to have a duty of confidentiality for information on any person who can be identified directly or indirectly by reference to name or any personal data [5].

For the HSE-related commitments of hospital consultants and other HCPs, the organisation is overseeing and enacting the recommendations imposed by GDPR. Nevertheless confirm with the appropriate authorities through proper documentation by letter/email prior to any personal or medical data of patient is requested to be released. It is inadvisable to share patient's personal data or clinical information to external sources without the explicit and written consent of the patient. Avoid storing, analysing and transmitting patients' personal data or medical information on non-HSE owned and non-encrypted peripherals such as laptops, mobile phones and tablets. If the primary location of work is a non-HSE hospital, ensure that their GDPR recommendations related to patients are fully complied.

Private medical practice: A private medical practice, in addition to being registered as a self-employed/sole trader/company, and having the Medical Council registration and indemnity, must register with the Data Protection Commissioner also as per the new GDPR norms [1, 2]. This is relevant if you are collecting, logging, storing and transferring PD or SCPD of patients. It is important to keep a paper trail of all steps taken towards GDPR compliance including the initial creation and review of an inventory list of patients and data points. It is important to streamline procedures to safeguard the personal data of patients [6]. Someone in the practice must be responsible for data protection compliance, a designated Data Protection Officer (DPO). Many GP practices already have a designated DPO [6]. I have developed a template (Appendix) that is going to be attached to the first appointment letter that is despatched if the child is referred to my private practice by a general practitioner (GP), another hospital consultant, public health nurses (PHN) or even for a self-referral.

Clinical research/clinical audit: The GDPR introduces protections for data subjects that aim for consistency across the EU including clinical and translational research areas [7–9] Research norms remain unchanged regarding informed consent, ethical guidelines and confidentiality. For patients from HSE hospitals, guidelines as set out by the Research Ethics Committee and Hospital Audit Committee are followed. If a patient who is only attending private practice is entered on to a clinical research or audit, a separate informed consent will be obtained. An explanatory memorandum for patients is shown in Appendix. If any general data/clinical pictures are logged, stored or transmitted (*portability of data*) for research, all the required ethical commitments to be fulfilled and data to comply with the GDPR norms. For individual cases worth publishing for important clinical learning, obtain the consent. Totally anonymised personal data is not coming under GDPR laws, however non-anonymised or pseudo-anonymised (pseudonymised) [3, 7] will and if a clinical researcher is holding or planning to hold such information they should have GDPR compliance.

The websites of Irish Medical Council and HSE offer guidelines as to how *they* are complying with GDPR but detailed guidelines for doctors is lacking [5, 10]. Irish College of General Practitioners (ICGP) website is more informative with a guideline for GPs already published [6]. The guideline is made up of three parts: the principles of data protection, frequently asked questions and appendices that provide forms and templates [6]. Other specialist professional colleges should follow suit and suggest interpretation, implementation and guidance for GDPR compliance [11].

While waiting for more authoritative recommendations, any registered medical practitioner could consider using the template that is included in Appendix for own practice. The document must be modified and adapted to individual practices.

Acknowledgements Author acknowledges the clarifications and guidance provided by Irish Data Protection Commission office and HSE Data Protection Office when contacted over the phone.

Compliance with ethical standards

This article does not contain any studies with human participants or animals performed by the author.

Conflict of interest The author declares that he has no conflict of interest.

Appendix

Date: 25/05/2018

Patient Reference Number:

Dear

With the introduction of the General Data Protection Regulation (GDPR) on 25 May 2018, the law on data protection is changing. As a healthcare professional practicing in Ireland, I have to let you know how we protect, use and store your child's personal and medical data. We will treat your information with respect and are committed to retaining the least amount of data required, proportional to the purpose. By accepting and attending the private clinic appointment you agree that we may process your child's personal data and clinical information in accordance with these terms.

Please read the information and if you have a query about how we handle your child's personal and medical data, you can get in touch via the contact details below.

Yours sincerely
.....
.....
.....
.....

IMC No:

1. What information do we collect about your child?

Summary:

Our private medical practice collects information that you provide directly to us such as through face- to-face visits at clinics, telephone calls to our practice, our website, other digital channels and/or from other sources such as our third-party providers [General practitioners (GPs)/ Public Health Nurses/ Other Consultants].

The personal information that we may collect includes:

- Name
- Email and mailing address
- Contact phone numbers – home / mobile
- Date of birth
- Gender
- Medical Records Number (if available)
- Contact preferences
- Name of your GP and contact address

2. What do we do with your child's personal and medical information?

Summary:

Our private medical practice uses your child's personal and medical information to provide him / her with appropriate medical care. We use the personal information of your child to manage our professional relationship with you, including planning, organising and reviewing clinic appointments / investigations.

These Purposes May Include The Following:

- Laboratory and Radiological investigations
- Onward referrals to other healthcare professionals / hospitals
- Treatment planning and prescriptions
- Follow-up arrangements
- Providing information about immunizations and age appropriate preventive and safety information.
- Our research initiatives and opportunities if available to participate (only after securing appropriate informed consent).
- Responding to requests for information from mandatory child protection agencies / regulatory bodies and upholding medico-legal obligations.
- Practice audits for compliance and managing day-to-day operations; and
- any other purposes that we may disclose to you from time to time.

3. Combining your child's medical and personal information:

Summary:

To provide your child with appropriate care and to personalise our services and interactions we combine information that we have collected about your child with professional information gathered from other sources.

Examples of these other sources include:

- External sources of healthcare provider information – from GPs, Hospital discharge letters, Hospital consultants, Allied health professionals, School reports.

4. Sharing your child's medical and personal information:

Summary:

We may share your child's clinical and personal information with other healthcare professionals / hospitals. / Schools and regulatory as well as child protection authorities as and when required.

We may share your child's personal and clinical information with:

- Your child's registered general practitioner (GP), public health nurse, other hospital consultants to whom the child requires onward referral, other hospitals for additional treatments and to any other healthcare professional or organisation that we may disclose to you from time to time.
- Regulatory as well as child protection authorities -as and when required, thus complying with the applicable laws and regulations.

5. What we don't use the personal information and your child's clinical data for:

Summary:

Disclosure to third parties without your explicit and specific consent (other than those mentioned in the above list in section 4).

We do not:

- Sell your child's personal or clinical data
- Share beyond the above mentioned statutory obligations without your permission
- Share third party details to you for marketing

6. Contact us

Data Controller and Data Protection Officer

..... is the controller of your child's data and personal information. Contact details of the data protection officer (DPO) are as follows: .....

GDPR Contact Information

Please address any questions, comments and requests regarding this Privacy Statement to .....Please ensure you quote the ID number at the top of this letter for security purposes.

General information on GDPR is available at https://www.dataprotection.ie/docs/GDPR or www.GDPRandYou.ie

References

1. Data Protection Commission www.dataprotection.ie/docs/GDPR (Accessed on 24th May 2018)
2. General Data Protection Regulation 2016/679/EU https://www.eugdpr.org/ (Accessed on 20th May 2018)
3. Murphy JFA (2018) The General Data Protection Regulation (GDPR). Ir Med J 111(5):747
4. European Society of Radiology (2017) The new EU General Data Protection Regulation: what the radiologist should know. Insights Imaging 8(3):295–299
5. Health Service Executive (HSE) www.hse.ie/eng/gdpr (Accessed on 24th May 2018)
6. Irish College of General Practitioners (ICGP) www.icgp.ie/data (Accessed on 18th May 2018)
7. Rumbold JM, Pierscionek B (2017) The effect of the General Data Protection Regulation on medical research. J Med Internet Res 19(20):e47
8. Chassang G (2017) The impact of the EU general data protection regulation on scientific research. Ecancermedicalscience 11:709
9. Cornock M (2018) General Data Protection Regulation (GDPR) and the implications for research. Maturitas 111:A1–A2
10. Medical Council of Ireland www.medicalcouncil.ie (Accessed on 24th May 2018)
11. McCall B What does the GDPR mean for the medical community? Lancet 391(10127):1249–1250. https://doi.org/10.1016/S0140-6736(18)30739-6