GET READY NOW FOR IMPORTANT CHANGES IN DATA PROTECTION

The European Union has ratified a data protection law – ECU Secretary General Ian Beesley explains how it might affect chiropractors.[12]

After 4 years of debate, the European Union has ratified a new data protection law (Regulation (EU) 2016/679). In George Orwell's *1984* the fear was of Big Brother physical surveillance. With the rise of the internet, email, smartphones, and tablets there has been an exponential and unprecedented growth in personal data such that Big Data is increasingly the basis for marketing, profiling and the development of sophisticated algorithms for determining action. The new Regulation responds to these developments by significantly altering existing law to give the individual more control of their personal data held by businesses. It will automatically come into force on 25 May 2018 without any further action by member states – though in the case of health there will be some opportunities for national authorities to supplement the requirements. Every organisation which handles personal data will have to comply with the new law and will have to demonstrate that they have complied (including all organisations in countries outside the EU if those countries want the ability to market and sell to the internal market). The law looks set to become the de facto world standard for data protection.

Personal data are defined as 'any information relating to an individual, whether it relates to his or her private, professional or public life;' and data processing is defined as 'any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.' So the management of patient records is within scope of the new law.

The regulations cover consent, management and use of data. Some of the changes are quite fundamental and will require chiropractors and clinic managers to re-evaluate how they deal with personal data about their patients and their employees. A two year transition period might sound generous but it is important to start planning soon for the new environment as re-configuring the management of existing personal data can be burdensome.

Consent

Independent research suggests that currently individuals often don't know if they have given consent to the collection and retention of personal data or to data being sold or used in profiling. In future it will be necessary to obtain unambiguous and explicit consent that is freely given for the specified use of personal data and can be just as easily reversed. (For those under 16 years the consent of a parent or guardian is required.) Silence, pre-ticked boxes or inactivity will not constitute consent. Only data that are necessary for the service provided will be regarded as freely given and even then the individual must have genuine free choice and the ability to withdraw or refuse consent without detriment. (Not all is at risk, however, as there is evidence that the more personal the service on offer the more likely that individuals expect to provide personal information.) Also, when consent is obtained the individual must be advised of the duration for which the record will be kept.

In addition, (s)he must be informed of the purposes for which the personal data are intended as well as the legal basis for it; the right to request access to and rectification of personal data or a restriction on how it may be used; the right to data portability (see below for further details); the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal; the right to lodge a complaint with a supervisory authority; whether the provision of personal data is a statutory or contractual requirement, as well as the possible consequences of failure to provide data; and the existence of any automated decision-making that may be based on the data, including profiling, with meaningful information about the logic involved, significance and envisaged consequences of such profiling.

---

[1] This article reviews material in briefing papers from the NHS European Office (www.nhsconfed.org/europe), DataIQ (www.dataiq.co.uk - General Data Protection Regulation, Identifying its impact on marketers and the consumer's moment of truth), Allen & Overy (www.allenovery.com The EU General Data Protection Regulation), and *Computer Weekly* (www.computerweekly.com/opinion/Proposed-EU-Data-Protction-Regulation-what-should-companies-be-thinking-about).

[2] An earlier version of this article was kindly subjected to peer review by Laura Fratelli (AIC lawyer), Satjit Singh (CEO BCA), Reem Bakker (Chairman ECU EU Committee) and Richard Brown (Secretary General WFC). I am very grateful for their help but any mistakes remain my responsibility.

However, the right to data erasure (the so-called right to be forgotten) does not apply to an individual's health record, or when personal data are used for public health or research purposes. Nor can the individual refuse access by professional bodies in the 'prevention, investigation, detection and prosecution of breaches of ethics for regulated professions.'

Clinics need to track when, where and what they have asked for in consent. At a minimum they should date and time stamp every record created, whether paper based or electronic. The burden of proof that consent has been freely given will lie with the record holder. If a patient finishes a course of treatment within the period of retention for their data and then returns later, consumer research indicates that three-quarters of people will expect consent to be sought again. .

Overall, across all providers of goods and services, individuals are six times more likely to agree to first party use of their data than to their details being passed to a third party (only 5% readily agree to this). The new law requires separate consent to be obtained for first party business use (for example, the ECU writing to those who have attended a recent convention with details about a forthcoming event) and for more generic marketing use such as from seeking consent to pass email addresses to exhibitors.

Data management

Clinics will need to review their privacy and data retention policies and how those policies are promulgated to staff and to patients. The language will need to be clear and uncomplicated. The statements will need to be prominently displayed and attention drawn to them (including proof that this has been done, such as by the individual ticking an appropriate box agreeing to the terms). Standard icons are under preparation in the European Commission that will be able to be used by clinics to symbolise that no personal data are passed to third parties

The underlying concept in the new law is that the patient is entrusting you with their data for safe keeping. It is your responsibility to have effective technical and organisational measures to ensure the security of data and to monitor how data are used. Large businesses (i.e. those that process more than 5000 records) will be required to appoint Data Protection Officers who will have personal responsibility for the organisation complying with the new rules.

At bottom, the new law requires those who hold personal data to adopt an approach based on the likelihood and severity of the risk of holding erroneous data and of a breach of data confidentiality. Consumer research (across all industries) points to 70% of people expecting their personal details held by businesses to be right every time and over half saying that the details are regularly wrong or misspelt (often errors in the recording of postal addresses). Hence the Regulation gives the citizen the right to access and correct the personal information held about them.

The Regulation also introduces a new right, to data portability. This could mean clinics being asked by patients for electronic personal data in an appropriate form so that they can choose to go to another provider of care (not necessarily a chiropractor). Data holders will be required to respond to requests for access to the individual's personal data normally within one month (and without charge). There may be a spike in requests as the new law comes into force and is tested – putting pressure on staff and on how proof of identity will be required and an audit trail established.

The preferred approach is to design data protection into procedures from the outset, involving a wide range of staff. Though data breaches should be rare clinics do hold sensitive personal information and should have a breach notification plan – what type of data you manage, where it is and who will co-ordinate the media response, customer communications and remedial action in the event of a breach. Should that happen, what types of information have been compromised? (A recent breach in a telecommunications company brought widespread anger when the company said that it could not be sure what had been compromised.)

The same consumer research indicates that just over half of citizens (57%) accept an obligation to help keep records up to date by reporting changes in their circumstances – though there is strong resistance to sharing changes between organisations. (BACKspace distribution, for instance, suffers from failures to do so with significant extra postal charges.) 43% are reported open to being asked to validate their data periodically and 29% every time they use a service. With a shelf life for holding personal data clinics may wish to put in place procedures for checking addresses electronically with patients and renewing permissions to hold the data.

Restrictions on use

Consent to using personal data for profiling will become a new requirement and patients will be able to object to their data being processed for direct marketing. This may give rise to a grey area concerning whether it is legitimate to profile patients and use this information to invite them to take up wellness or check-up consultations. It seems likely that this will only be legitimate against an explicit consent (renewable at six monthly intervals) that recognises the patient's right to question and fight decisions that affect them that have been made on a purely algorithmic basis.

ACTION PLAN

In summary, what actions should chiropractors now consider in the light of the new law:

1. Review data protection/privacy policies to ensure that they are clear and accessible
2. Review whether documents and forms of consent comply with the need for affirmative action
3. Review processes for pseudonymisation or anonymization of patient records
4. Review how you provide information to patients during care
5. Review data retention procedures
6. Review procedures and monitor requests for access to a patient's data
7. Review how you will establish audit trails
8. Check that consents that will last until the law comes into force have been freely given, are explicit and informed – it will be your burden of proof
9. Conduct an impact analysis and prepare for breaches
10. Plan awareness training for all clinic staff
11. Stay in touch with your national association over specific developments to be introduced by your national healthcare authorities

[END]