M. Lovell
M. Lovell, FRCS (Orth), Consultant Orthopaedic Surgeon, Manchester University Foundation Trust

M. A. Foy
M. A. Foy, FRCS, Consultant Orthopaedic and Spinal Surgeon
foyfrcs5@gmail.com

General Data Protection Regulation May 2018 (GDPR): how does it affect us?

Readers are no doubt aware that from 25 May 2018, changes to the way we handle data in the NHS and in both private and medico-legal practice have come into law. Strangely, as we move towards Brexit, the 1998 Data Protection Act has been replaced by the General Data Protection Regulation (GDPR), which is based on an EU directive to standardize the collection and processing of data on EU citizens in the UK, Europe, and the rest of the world.[1,2] According to the Medical Defence Union (MDU, 2018), Brexit is not expected to affect its implementation and the intention is that when the UK leaves the EU, it will be incorporated into UK domestic law under the European Union (Withdrawal) Bill, currently before parliament. Most, if not all, of us who practice outside the NHS will already be registered with the Information Commissioner's Office (ICO) under the 1998 Act, and will be paying the annual fee of £35 that is levied to organizations that hold personal data but employ fewer than 250 people.

Making clinical records regarding our patients, and retaining them for certain minimum periods of time, is part of our clinical duty. Ensuring that patient records are kept safe is also a legal requirement. From a medico-legal perspective, protection of claimant data and records is just as vital. In the event of a complaint, claim, or regulatory action, our clinical records are the first line of defence. Without them, it is extremely difficult to prove how the patient presented when assessed clinically, what our advice or warnings to the patient were, and what precise treatment was discussed, offered, or provided. Even if we happen to remember the patient and our consultations clearly, courts and tribunals are extremely reluctant to rely on a clinician's recollection if there is no documentary evidence to back it up.

Under the GDPR, the responsibilities associated with holding personal data have been made much more onerous and rigorous. It requires organizations of any size that process personal information to adhere to these new standards. You, through your sole tradership or limited company, will undoubtedly be a Data Controller for some, and perhaps all, of the data processing that is carried out in your clinical practice. You or your business entity will be a Data Controller if it determines the purpose for, and means by which, data is processed. It will also be a Data Processor for information that is dealt with under the direction of another organization or individual, such as a medico-legal agency, a firm of solicitors, or an insurance company who instructs you as an expert witness in a claim. A Data Processor is someone or a company that manages, stores, modifies, or analyzes personal data, on behalf of a Data Controller.

An orthopaedic surgeon treating private patients is likely to be a Data Controller rather than a Data Processor. However, a medico-legal expert is likely to be a Data Controller for some data and a Data Processor for other data. The GDPR requires both Data Controllers and Data Processors to ensure that compliance procedures have been put in place. In particular, orthopaedic surgeons should ensure that any third party with whom data is shared is GDPR compliant and that all their employees are aware of GDPR.

The GDPR means that Data Controllers and Data Processors need to consider if they must appoint a Data Protection Officer (DPO). This is an individual responsible for ensuring your firm has GDPR-compliant systems. Given the fact that most orthopaedic surgeons practise either as sole traders or through their own limited company, the appointment of a DPO may be considered somewhat excessive! However, someone in the office should be nominated as

DPO. That person could then help ensure, if you are a Data Controller, that your firm pays the Data Protection Fee, which replaces the Data Registration Fee, to the Information Commissioner. They should also ensure your firm has good data protection procedures in place including data security and staff training, ensure that any 'Subject Access Requests' are handled properly, and ensure that reports to the ICO concerning any breaches of security that is likely to result in a risk to the rights and freedoms of individuals are reported within the 72-hour reporting deadline.

Whoever in the office is responsible for GDPR compliance must determine what information the sole tradership or limited company holds. This will probably include:

- Written/typed/electronic records (including medical records and medico-legal reports/ correspondence);
- Databases of present and former customers, which will include medical insurance companies (Bupa, Axa PPP, Aviva, Cigna etc), instructing solicitors, and instructing insurers;
- Staff HR details if appropriate;
- Financial records; and
- Possibly marketing databases, if you have sent out emails or hard-copy marketing literature to local GP surgeries or solicitors.

Orthopaedic surgeons need to assess the risk attached to the information that they hold. These risks will include possible security breaches, improper processing of information – for example, using patient details for marketing without consent – or failing to get rid of personal data when it is no longer required.

This latter issue is a thorny one in terms of retention of patient records and medical reports. The advice from professional organizations is conflicting. The guidance for private practitioners is contained in the Private and Voluntary Health Care (England) Regulations 2001 (schedule 3). This sets out minimum retention periods for minors and adults. The advice for those aged 17 years or under is to retain until the patient is 25/26 years old. For all other patients, the recommendation is eight years from the date of the last entry in the record. This does not sit easily with the GDPR focus on data minimization, with data only being processed for limited and legitimate purposes, and stored for no longer than is absolutely necessary for those purposes. With this in mind, some consideration should be given to retention periods in your particular practice. It would be good practice to create a policy document for your private and medico-legal practice, identifying the applicable retention periods, with the aim of ensuring that the records are kept for as long as necessary, but no longer.

Therefore, only collect information that you need for a specific purpose, keep it secure, ensure it is relevant and up to date, only hold as much as you need for as long as you need it, and allow the subject of the information to see it on request. To reflect the conflicting advice available (bearing in mind the recommendations of the 2001 Act), discussion with the ICO helpline by one of us (ML) was conducted for advice on how long we should keep information for. They do not stipulate a minimum or maximum time period, but it appears that we have to justify why we are retaining data that may include patients' notes or our reports and handwritten notes. It may be that patients' notes can be destroyed fairly promptly, although it has always been the practice of one of us (MF) to retain them for three years. Some medico-legal agencies are suggesting six months for disposal of medical records. We are concerned at this advice and our practice is to retain records while the claim is ongoing and destroy confidentially when informed that the case has settled. This, of course, raises another issue, in that many solicitors and agencies fail to tell the expert that the case has settled. This may be facilitated by better communication between the orthopaedic expert and their instructing party from the commencement of the case, but may also require review of outstanding files and communication with the instructing party periodically. For the actual medical reports, recent advice from medical defence organizations has suggested a period of ten years for retention of reports and hand written notes. We find this difficult to comprehend in light of the GDPR requirement to retain personal data only for as long as it is required, particularly if a claim has settled.

It is also important under the GDPR to ensure that cybersecurity is up to date. Cyber security comprises technologies, processes, and controls that are designed to protect systems, networks, and data from cyber attacks. Effective cybersecurity reduces the risk of cyber-attacks, and protects organizations and individuals from the unauthorized exploitation of systems, networks, and technologies. Access to any Wi-Fi that you use should be secure. Backups of electronic files need to be made. We understand that malpractice insurance companies such as ISISIS (now Incision) are planning to include cybersecurity protection in their annual cover.

In your role as a Data Processor, it is likely that any agency, solicitor, or insurance company that instructs you as an expert witness will require you to adhere to the following:

- All data sent to you is documented and deleted when there is no longer any legal or contractual need to retain it;
- All data is stored and transmitted securely;
- No data is shared with or passed to any other party without their permission;
- That you/your organization has reviewed its internal data protection procedures and information security processes and controls in line with the GDPR; and
- That you are not using data provided to you for your own marketing purposes (without the consent of the subject) and are only using it for the purpose that it was sent to you.

Any breaches are reported to the Data Controller (at the agency, solicitor, or insurance company) immediately, as the Data Controller is now bound by the GDPR to report this to the ICO and the subject within 72 hours. According to the ICO, failure to do so may result in a fine of up to 10 million euros or 2% of the organization's annual turnover, whichever is greater.

The ICO website has prepared a useful guideline outlining 12 steps that should be taken to incorporate the GDPR into your current security arrangements. They point out that many of the GDPR's main concepts and principles are much the same as those in the current Data Protection Act (DPA), so if you are complying properly with the current law then most of your approach to compliance will remain valid under the GDPR and can be the starting point to build from. However, there are new elements and significant enhancements, so you will have to do some things for the first time and some things differently.

They emphasize that it is important to use their checklist and other ICO resources to work out the main differences between the current law and the GDPR. The ICO is producing new guidance and other tools to assist as well. The GDPR places greater emphasis on the documentation that data controllers must keep to demonstrate their accountability. Compliance with all the areas listed in the guidelines will

require orthopaedic surgeons to review their approach to governance and how they manage data protection as a 'corporate' issue. One aspect of this might be to review the contracts and other arrangements you have in place when sharing data with other organizations.

How do we apply all this from a practical perspective? Some specific queries have been raised by BOA members:

Can medical reports containing confidential data still be sent by post? Should the post be registered? We see no major difference between the medical report and the letter from consultant to GP or from hospital to patient, and would see no reason why this practice cannot continue.

Can medical reports/patient letters be emailed or do they now need to be encrypted or password-protected? We believe that with the advent of GDPR and the general concerns regarding cybersecurity, communications containing confidential patient/claimant data sent over the internet should be encrypted or password-protected. It would be difficult to defend if there was a leak of such information. Those of us who use electronic databases or digital dictation systems where confidential medical information is transferred over the internet have found that the companies responsible for these systems have introduced such encryption. In the case of one of the authors (MF), this has been introduced by Bluespier and Dscribe, respectively.

What is the best method of disposing of medical records? We would recommend that paper records are disposed of via a secure shredding company. This will have cost implications but is required following the GDPR. Electronic records can be deleted directly or in liaison with the administrator managing the database (e.g. Bluespier).

In medico-legal practice, can we still email draft joint statements following telephone discussions on cases, or should they now be password-protected or encrypted? We believe that if they contain confidential medical information, password protection/encryption is required. At the draft stage, they can, of course, be anonymized.

In summary, you have to show that you comply with the data protection principles, i.e. that personal data is processed lawfully, fairly, and in a transparent manner. Personal data must be collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with that purpose, for example being sold on to data-mining companies. The collection of personal data must be adequate, relevant, limited to what is necessary, accurate, and kept up to date. It must not be kept for any longer than is necessary and it must be kept secure. The GDPR also requires you to be able to demonstrate that you have complied with these requirements. You should therefore have adequate data processing records. To keep this personal data, you will need the explicit consent of the data subject (patient/claimant) and show that the holding of such data is necessary to protect the vital interests of the data subject.

Times have changed. The days are gone when private and medico-legal practices can be run as a cottage industry with files on the floor of the NHS secretaries' office. In reality, the great majority of us have already moved with the times, but we now have another challenge/legal requirement to deal with in our practices with the advent of GDPR. However, just as with any new law, there will inevitably be a period of uncertainty until the full practical implications of the new requirements become clear, and reliable guidance emerges in response (for example, from the ICO or the General Medical Council (GMC)). It may take even longer for disputes arising out of the new law to be decided by the Courts and become precedents to provide clarification. Accordingly, we should not treat 25 May 2018 as the end of our work to become GDPR-compliant, but the beginning. Adapting our processes and procedures to respond to updated guidance as it emerges is likely to be necessary for months and possibly even years to come.

REFERENCES

1. No authors listed. General Medical Council. The General Data Protection Regulation and the Data Protection Bill 2017-19. 2018. https://www.themdu.com/guidance-and-advice/guides/the-general-data-protection-regulation-and-the-data-protection-bill-2017-19 (date last accessed 14 June 2018).

2. No authors listed. Information Commissioner's Office. Preparing for the General Data Protection Regulation: 12 steps to take now. 2018. https://ico.org.uk/media/for-organisations/documents/1624219/preparing-for-the-gdpr-12-steps.pdf (date last accessed 14 June 2018).

 DOI: 10.1302/2048-0105.74.360622