Data protection and the eLogbook

AT Vesey British Heart Foundation Centre for Cardiovascular Research, University of Edinburgh
JEF Fitzgerald Royal College of Surgeons of England, Association of Surgeons in Training
A Lamb Royal College of Surgeons of Edinburgh

The pan-specialty surgical eLogbook, maintained by The Royal College of Surgeons of Edinburgh (RCSEd) on behalf of the four royal surgical colleges, is now the de facto tool for all surgical trainees. The colleges issued new terms and conditions at about the same time that general surgical trainees were obliged to transfer to the eLogbook from the previously mandated Intercollegiate Surgical Curriculum Programme logbook. Some of the clauses within the terms and conditions gave rise to concern, and several trainees contacted the Association of Surgeons in Training (ASiT) to seek clarification.

In this article, we have undertaken to briefly review the most pertinent legislative background and to address the concerns that arose. Data governance in medicine is a large, expanding and complex issue and this monograph sets out to achieve a balance between protecting the rights of the individual to maintain control of their personal data and the rights and responsibilities of those who hold and control that data.

In an attempt to strike this balance, much legislation has been drafted and enacted in the EU and the UK during the past 30 years. The most recent and germane piece of UK legislation is the Data Protection Act (DPA) of 1998.

The Data Protection Act 1998

Key Definitions

> Data subject – the identifiable individual to whom personal data pertain.
> Data controller – any entity (individual or organisation) that determines how personal data are processed.
> Personal data – any data that can be linked to a living individual. This definition also applies to pseudonymised or linked-anonymous data when the data controller has the means to ‘decrypt’ such data.
> Sensitive personal data – any personal data relating to race, ethnicity, political opinion, religion, health, sexual life, actual or alleged criminal record.

Although complex, the DPA in essence ensures that personal data is handled correctly. It sets out to achieve a balance between protecting the rights of the individual to maintain control of their personal data and the rights of organisations to use such data legitimately without undue regulatory stricture.

It achieves this in two ways: first, the act places certain obligations upon data controllers and, second, it enshrines certain rights for data subjects (that mainly relate to data access, quality and use). The whole act is based upon eight principles:

1. Personal data shall be processed fairly and lawfully.
2. Personal data shall be obtained only for lawful purposes.
3. Personal data shall be adequate, relevant and not excessive.

4. Personal data shall be accurate and up to date.

5. Personal data shall not be kept for longer than is necessary.

6. Personal data shall be processed in accordance with the rights of data subjects.

7. Data shall be held and processed securely.

8. Personal data shall not be transferred to another country without adequate protection.

A key theme is consent. In most cases, the consent of the data subject should be sought before processing personal data. In the case of sensitive personal data, obtaining 'explicit consent' is nearly always mandated. Individuals or organisations acting as 'data controllers' must be registered as such with the Information Commissioner's Office (ICO).

The DPA and the eLogbook
The eLogbook is a large database holding vast amounts of apparently sensitive personal data pertaining to millions of people. In order to ensure full compliance with the DPA, a number of measures were instituted including the release of the aforementioned terms and conditions. It should be noted at the outset that the actual servers that host the eLogbook (and ISCP databases) are housed and maintained by a company with the appropriate expertise that has a contract with the colleges and the Joint Committee on Surgical Training.

Here follow the clauses that gave rise to concern, accompanied in each case by a brief analysis and answer.

A link to full terms and conditions can be found at the end of the article.

Clauses 1.8, 11.1, 12.1 and 12.7
These clauses relate to the colleges' and users' obligations as stakeholders in the eLogbook. The colleges, as administrators of the logbook, are clearly defined as data controllers as specified by the DPA but it is not necessarily clear whether users should similarly register with the ICO as individual data controllers.

Two points are relevant. The first relates to the individual user's employer. As an NHS employee or indeed a university-employed research fellow, an individual will be required to process sensitive personal data on a daily basis and therefore will qualify as a data controller. Strictly, in these instances, the employer will have notified the ICO and therefore the employee is in theory automatically 'covered'. If, however, any data is 'privately' collected and processed then an individual is not covered by the employer's notification.

The second point relates to whether data collected on the logbook actually count as 'personal data'. It could be argued that they do not as no immediately identifiable information fields are completed. However, referring to the definition of personal data, if the data controller in question has the means to link 'anonymous' data back to an individual (easily done with a Community Health Index or hospital number) then such data do indeed qualify as personal data and a user should notify the ICO. Furthermore, in the case of 'sensitive personal data' (ie all the data on the logbook), explicit and informed consent should also be obtained before collecting such data. Given that failure to comply with the obligations as set out by the DPA constitutes a criminal offence, should all users of the eLogbook therefore register with the ICO as data controllers and obtain 'explicit and informed consent' for every patient they operate on? Is this realistic?

The royal surgical colleges' legal team has confirmed that those who record or use personal data or sensitive personal data in a 'self-employed capacity' (ie outside of their employment with the NHS or universities) will need to be notified with the ICO as data controllers. Given that most trainees will at some stage assist their consultant trainers in the private sector and that many will train within independent sector treatment centres (ISTCs) outside the NHS, registering with the information commissioner as a data controller should be regarded as mandatory. Furthermore, data collected, processed and retained by an individual during a period of transient employment with a university (ie as a research fellow) may also fall out of the remit of the universities' ICO notification once such employment ends. This should be regarded as another absolute indication for individual notification. It should, however, be noted that personally retaining non-anonymous (ie linked-anonymous or pseudonymous) personal research data on laptops or personal computers is not advisable. If strictly necessary, these data should be properly encrypted.

Gaining written, explicit consent from 'private' or ISTC patients for collecting logbook data is a must. Although it is the case that this is not strictly necessary for NHS patients, there is a strong deontological argument for doing so; the standard should apply to all patients.

Gaining such consent is also consistent with the spirit of the DPA as well as General Medical Council guidance on the matter. A trainee should always meet a patient before participating in their surgery. Most consent forms now have a field relating to data collection and audit; a few extra words about the need to maintain a logbook for training shouldn't represent a significant burden.

Clause 6.3
'To the fullest extent permitted by law, we shall not be liable, including for any indirect, special or consequential loss or economic damage (such as without limitation loss of bargain, profit, data, reputation, placement, position, learning agreement, resultant losses or otherwise), and whether in contract, tort, or otherwise, arising out of the use of the website or the reliance on any of the information displayed on it.'

This clause limits the liability of the colleges for user activities. There had been concern that this was a way of limiting the colleges' liability in the event of data loss (by the website) and the professional difficulties for the user that would arise as a consequence.

The royal surgical colleges' legal team have given assurances that this does not relate to data loss but rather the quality of the data on the website.

As the colleges are not themselves entering patient data, data are ever-changing and there is an ever-present
risk of illegitimate access, it is evidently not possible to track and quality control all of the content all of the time. The colleges therefore cannot reasonably be expected to assume liability for illegal or irresponsible use. The surgical colleges’ legal team have emphasised that user liability would only arise if such a breach had occurred as a result of the user’s own failure to take ‘reasonable security steps’ (for example, not disclosing passwords, etc). Individuals would not be liable were the colleges or some other entity at fault. The team also noted that enforcement actions and fines for breaches of the DPA are unlikely to arise unless there has been substantial damage and distress caused as a result (for example, loss of a large database of personal data).

Clause 12.3
‘Special care must be used when inputting data in any free fields, including for “other information” accordingly.’

Questions arose relating to which data this referred to. The formal advice is to strictly avoid inputting any data that might link the entry to an individual (addresses, telephone numbers, names). Further clinical or operative details are acceptable.

Notifying the ICO of status as data controller
This can be done online by using the links quoted at the end of the article. There is a self-assessment tool that will recommend notification. The ‘New Notification’ icon needs to be selected and instructions will follow. There is a specific template for junior surgeons using the eLogbook (N955) to follow. The annual fee is £35.

Summary
The obligations placed upon individuals by the DPA are strict and probably not appreciated by many eLogbook users. All trainees are strongly advised to notify the ICO of their status as data controllers.

Gaining explicit, informed and written consent to collect data for the purposes of logbook maintenance should now be encouraged.

Maintaining a detailed personal logbook of operations with outcomes will appeal to many trainees and is an aim that should be commended. Caution is advised, however – individuals should ensure that they are notified with the ICO, familiar with the DPA and encrypt the data adequately.

Useful links
Intercollegiate eLogbook Terms and Conditions: www.elogbook.org/site/2903/default.aspx
How to notify the Information Commissioner’s Office: www.ico.gov.uk/for_organisations/data_protection/notification.aspx
Association of Surgeons website: www.asit.org and @ASITOfficial on Twitter

MSc in Translational Cardiovascular Medicine

A distance e-learning programme (full time: one year, part time: two years) delivered by clinicians and scientists and designed to appeal to a wide range of students.

It includes three two-week residential workshops, which will be held in Bristol, United Kingdom, for hands-on experience and assessments.

For more information, visit:
www.bris.ac.uk/prospectus/postgraduate/2013
or email Professor Sarah Jane George:
socscardiology-msc@bristol.ac.uk

University of BRISTOL

APPLY TODAY