Information Governance in Dental Practices

Summary of findings from ICO reviews

September 2015

Executive summary

The Information Commissioner's Office (ICO) is the regulator responsible for ensuring that organisations comply with the Data Protection Act 1998 (DPA) and for promoting good practice in information handling. The DPA consists of eight principles with which all organisations processing personal data must comply.

Between June 2014 and June 2015, we visited 21 dental practices across the UK in order to understand the information risks and challenges that dentists are facing. We also conducted an online survey and held discussions with the British Dental Association (BDA), the Medical Defence Union (MDU) and Dental Protection.

Our visits could only cover a small number of dental practices and were predominantly to practices in England, due to the practices who were willing to participate. Despite these limitations, we believe that there are common themes and challenges faced by dentists in complying with the DPA. These challenges are set out below.

Summary of findings:

- There is confusion around when a dentist should register with the ICO, with some dentists registering when it is not necessary, and others not registering when it is required.

- Dentists do not always have written contracts, with appropriate clauses about information security, in place with contractors, particularly IT contractors. There was also evidence that some of the risks of new technologies, such as working on mobile and personal devices, are not being appropriately controlled.

- Retention policies (to determine when records, both physical and electronic, should be destroyed) were not in place at all sites visited. Retention periods were not always clear, and not generally applied to electronic records.

- There was some evidence that dentists are not always engaged with sources of best practice and new guidance in relation to information governance.

Recommendations

1. Responsibility for compliance and registration

Under the DPA, those responsible for the processing of data are called data controllers. A data controller must be a "person" recognised in law, that is to say: an individual, an organisation or another corporate or unincorporated body of persons. Data controllers determine why and how particular personal data will be used.

Dentists operate within a number of different complex structures, including individual practices, partnerships, expense-sharing arrangements, limited liability companies and dental corporates. This has led to some confusion about the circumstances in which a dentist is (or is not) a data controller, responsible under the DPA for patient data, and also for registration with the ICO.

Most individuals access their dental care through a named dentist at their local practice. Payment is provided to the practice, and the patient will deal with the practice through its reception staff. The common perception is therefore that the practice is the organisation responsible for treatment and for data protection.

The actual picture of data controllership is far more complex.

It can be difficult to decide who is responsible for data protection in some of the above structures. This can be seen in the confusion amongst some dentists about who must register with the ICO (unless exempt, data controllers are required to register and then renew annually). It also leads to the risk that personal data is not protected properly because it is unclear who should be leading the work.

Whilst it is not possible to give a single rule that will fit every situation, there are a number of questions that might clarify whether a particular dental practitioner is a data controller.

1. Are you responsible for the control and security of patient records, and do you have other responsibilities associated with the data?
2. Do you have a patient list separately from the practice in which you treat patients, that would follow you if you left?
3. Do you treat the same patient at different practices?
4. If a complaint was made by a patient, or data was lost, would you be legally responsible for dealing with the matter?

If you answer 'yes' to any of the above questions, you are likely to be a data controller and will need to register with the ICO. You can register by visiting our website www.ico.org.uk and selecting the link on the front

page 'Register your organisation'. It will take around 15 minutes to complete. If in doubt, the ICO has a self-assessment tool and also specific dental practitioner FAQs, as well as a Registration helpline - 0303 123 1113.

Example 1

A self-employed associate dentist works across two practices, each led by a principal dentist. Although the principal dentists organise the premises and IT systems for their own practices, the associate also maintains their own laptop and dental treatment software. They are legally responsible for the records of the patients they treat, which are stored on their laptop and are taken from site to site. The patients treated by the associate may be treated at either of those sites. The associate is likely to be a data controller, and should therefore register with the ICO.

Example 2

A self-employed associate dentist works for a small practice, led by a principal dentist. The principal dentist organises the premises and IT systems. The associate treats only those patients who come to the practice, and does not treat patients at any other practice. When the associate leaves the practice, he does not take any patient data with him. The associate is unlikely to be a data controller, and therefore will not need to register with the ICO.

2. Information security arrangements

Information security is a wide-ranging topic. It covers everything from physical security of records and premises, to using firewalls and anti-virus software, to training staff appropriately.

Dentists have a number of requirements placed upon them in relation to maintaining the security and integrity of records. Beyond the DPA, the General Dental Council (GDC) publish Standards for the Dental Team; Principle 4 is to "Maintain and protect patients' information". Similarly, "Outcome 21: Records" of the CQC's Outcomes Framework outlines the controls against which dental providers can be audited.

Under the DPA, organisations must have appropriate security to prevent the personal data you hold being accidentally or deliberately compromised. In particular, the DPA requires data controllers to take specific steps when using a third party (a data processor) to process personal data on their behalf. The DPA requires that data controllers:

- choose a data processor providing sufficient guarantees regarding information security;
- take reasonable steps to ensure compliance with those measures; and
- have a contract in place, in writing, specifying that:
    - the data processor is to act only on instructions from the data controller; and
    - the data processor must comply with information security measures comparable to those in the DPA.

In most of the practices we visited, general information security was fairly good. Dentists and dental staff are trained healthcare professionals, and therefore understand the requirements of confidentiality. However, there were some areas of information security where many dentists struggled; notably, ensuring that third parties (such as IT contractors) were covered by an appropriate formal contract, and managing some of the new ways of working (through mobile or personal devices, or at home).

Data processor contracts

In many of the smaller practices we visited, information technology support was provided by small-scale IT contractors. The arrangements for the IT support were often informal, either not written down, or else amounting to a small service-level agreement. They rarely included clauses concerning information security measures.

In some cases, this was justified on the basis that the contractor was unlikely to have access to personal data (working with hardware under supervision, or installing software only to new equipment). Nevertheless, it remains a possibility that contractors would be able to access personal data in the course of their work.

Home and mobile working

Home and mobile working was not, at the time of our visits and survey, widespread in dental practices, although it did appear to be becoming more prevalent, with dentists reporting that they were aiming to have the facility available.

In those places currently using home-working, or likely to do so in the immediate future, few procedures had been implemented to control how patient data would be used. There were examples of:

- typing up patient notes at home and emailing them, or transferring them on USB memory sticks to their practice (sometimes encrypted, sometimes not);
- using pseudonymised or anonymised patient data for CPD;
- using third party remote access software to access practice systems through personal computers; and
- staff bringing their own personal devices to use at work for work purposes (Bring Your Own Device, or BYOD, as it has become known).

It is important that dentists should consider carefully the risks associated with the use of mobile and home working (although it is entirely possible to use these tools securely). For example:

- Do home computers have appropriate security software to prevent unauthorised access (by other users or if they are lost or stolen)?
- How are home computers destroyed at the end of life?
- Are USB memory sticks appropriately encrypted when transferring data (to prevent accidental loss)?
- Are USB memory sticks properly scanned to prevent the potential import of malware into practice systems?

The ICO information security page contains useful information about applying information security principles, as well as links to our BYOD and encryption guidance and a practical guide to IT security for small businesses.

3. Retention of personal data

The DPA states that personal data should be retained for no longer than is necessary. However, it does not go on to specify how long is necessary for different categories of personal data. The following questions therefore tend to be asked (in descending order of importance):

- Is there any other legislation that requires that personal data be retained (for example, for income tax purposes)?
- Are there any agreed industry standards for retention (for example, an industry regulator or association has established rules for bodies within the industry)?
- What is your organisation using the records for, and when is the soonest they will not be of any use?

In the case of dental records, the BDA have established the following recommendation for retention of dental records:

- 11 years for adults
- For children 11 years or up to their 25th birthday, whichever is the longer

The BDA took this decision based on the various limitation periods for bringing legal claims for personal injury, clinical negligence or breach of contract. These recommended retention periods are reiterated in the NHS Code of Practice: Records Management (which notes that they are derived from the BDA).

Not all dentists are members of the BDA, nor do all dentists provide NHS treatment. However, other industry bodies have tended to give broadly similar advice.

It should be noted that the discussed retention periods are maximum retention periods; that is, the length of time before records become unnecessary, and therefore, under the DPA, should be securely destroyed. There are very few circumstances in which retaining records indefinitely will be compliant with the DPA.

It should also be noted that there is some variance in retention periods across the UK. Although the UK DPA sets out no specific retention periods, the Regulation and Quality Improvement Authority (RQIA), Northern Ireland's independent health and social care regulator, has established regulations laying out particular retention periods for records (records should be kept for 10 years or until the patient reaches the age of 27, if they were 17 years old or younger when the treatment was provided). These retention periods are established as minimums; therefore, there is no conflict with the other retention periods previously discussed.

Many respondents did not know how long they were required to retain patient data, leading to a wide variety of practice. Industry bodies have designed standards, to which some dentists adhere for manual records. All dentists interviewed retained electronic records indefinitely.

Where practices had policies in place and followed them, they destroyed only manual or physical personal data. However, most practices are now moving to electronic dental records. None of the respondents to our research disposed of electronic records, or had the facility to do so.

The ICO recommends that dental practitioners implement a retention policy. A retention policy is a short document or schedule that lists when personal data should be destroyed, based on the questions and industry

standards discussed above. This means that there is an easy, accessible answer when asking if a given piece of information should be destroyed.

Retention periods apply to manual and electronic records. Although practices were archiving inactive patient records (according to the facilities of their systems), these records remained intact and accessible at the push of a button. It is important that the dental sector begins to consider the importance of securely destroying electronic records at the end of their retention period.

In the meantime, for practices which do not have the technical capability to delete personal data due to system constraints, our guidance on deleting personal data lays out some important principles for putting such information "beyond use". The data controller:

- is not able, or will not attempt, to use the personal data to inform any decision in respect of any individual or in a manner that affects the individual in any way;
- does not give any other organisation access to the personal data;
- surrounds the personal data with appropriate technical and organisational security; and
- commits to permanent deletion of the information if, or when, this becomes possible.

4. Engagement with the wider information governance landscape

All organisations must keep up-to-date with how to keep information secure. The way in which some practitioners are failing to adapt effectively to the new use of mobile and personal devices within the workplace highlights the importance of being alert to guidance and advice about using new technology securely.

Pressures on the time of dental professionals seeking to run their own businesses (still the vast majority of dental providers within the UK) mean they can struggle to engage with more involved information governance issues. There have been a number of examples of nationwide information governance projects (including this one) which have gathered responses from only a few dental providers.

Most dental practitioners are understandably focused on delivering care to their patients, and cannot spend large amounts of time addressing complex information governance matters. The ICO is pragmatic about the requirements of running small businesses.

The general response from the dental sector to this piece of work (and engagement with pieces of information governance work led by other organisations, to which the ICO was party) suggests that additional channels of communication with the sector would be valuable.

The sector has industry bodies (GDC, BDA, MDU and Dental Protection) as well as smaller web-based or geographically localised communities and sectoral press. Effectively marketing guidance messages using these channels will be key to improving the sector's responsiveness to new information governance challenges.

Further actions

The ICO has produced a range of guidance to help organisations manage and secure personal information. This guidance can be found on our website, ico.org.uk, with particular health guidance at ico.org.uk/health.

Other useful guidance

- A practical guide to IT security
- Bring Your Own Device (BYOD)
- Guidance on the use of cloud computing
- IT security top tips
- Retaining personal data

Advice and Assistance

The ICO's helpline can answer queries about data protection compliance and can be contacted on 0303 123 1113.

The ICO also has offices in Scotland, Wales and Northern Ireland which can answer questions specific to those legislation and regulations in those areas.

The Scottish office can be contacted on 0131 244 9001.

The Welsh office can be contacted on 029 2067 8400.

The Northern Irish office can be contacted on 028 9027 8757 or 0303 123 1114.

Appendix

Methodology

We invited a large number of dental providers to take part in our visit programme or complete our national survey (although only a fraction of the total; the August 2014 Care Quality Commission publication, "A fresh start for the regulation and inspection of primary care dental services", places the number of dental care locations at 10,102 in England alone). Visits were delivered to 21 practices, covering sole traders, partnerships, limited companies and members of dental corporates. Some practices offered private treatment only; others mixed NHS and private treatment. We visited (as far as possible given the voluntary nature of the visits) dental providers in different geographical regions.

Our visits took the form of a half-day, onsite informal review of the dental provider. We looked at how the organisation handled personal information, offered practical advice and guidance on relevant topics and provided a short summary after the visit. The visits typically covered information security, records management, training and requests for personal data. In a small number of cases we contacted the dental provider by phone to discuss these topics.

We also issued a national survey, asking dental providers a series of information governance questions. This was issued directly to a number of corporate dental chains and practices and indirectly through promotion by the BDA, MDU and Dental Protection. Despite the coverage achieved in this way (and the length of time the survey remained open), we received only 49 responses. Nevertheless, those responses agreed with the picture formed from our visits.

Finally, we approached three of the largest relevant industry bodies. The BDA, the MDU and Dental Protection discussed the current information governance challenges they identified as being most serious within the dental sector, and gave us access to the type of advice they are providing to their members.

We recognise the difficulties such a small response gives to effectively establishing what key risks face the dental sector. In addition to having insufficient respondents to recognise statistically significant trends, those practitioners that did respond will be subject to a volunteer bias; that is, one would expect that they are keen to engage with information governance, possibly leading to their practices having a better information governance baseline than the norm. However, we hope that the wide experience of dental sector challenges provided by the industry bodies will serve as a partial corrective to this problem.