Protecting patient data

David Lauder, dento-legal adviser at the Dental Defence Union (DDU), discusses the importance of data protection guidance and the responsibilities of dental professionals in protecting patent data.

GDPR legislation[1] defines a personal data breach as 'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed'.

In the case of dentistry, dental professionals are directly responsible for the data held on patients, and those who are data controllers in the practice must be registered with the Information Commissioner's Office (ICO).[2]

In Standard 4.5 of the GDC's *Standards for the dental team*,[3] it states that dental professionals must:

'Keep patients' information secure at all times, whether your records are held on paper or electronically. [Furthermore] you must make sure that patients' information is not revealed accidentally and that no-one has unauthorised access to it by storing it securely at all times. You must not leave records where they can be seen by other patients, unauthorised staff, or members of the public.'

Additionally, this is supported by Standard 1.3 which states that dental professionals 'must be honest and act with integrity'.

Storing patient data

While data controllers are primarily responsible for the security of patient data, individual dental professionals have an ethical duty of patient confidentiality and must keep patient data from being mislaid or accidentally disclosed. Failure to do so may result in a patient complaint or even a GDC investigation.

There are a number of actions that can be taken to protect patient data. Firstly, it is important to not store any identifiable personal data on personal computers or mobile devices, such as memory sticks, laptops, or personal mobile phones, which risk being misplaced or accessed by other people. If you need to work on confidential documents at home, discuss and agree what you can do with the data controller.

Next, it is vital that all staff are familiar with the workplace information security policy, including the name of the person in charge of data security.

Also, be aware of relevant guidance, such as that provided by the GDC and the NHS,[4] as well as your legal requirements to protect confidentiality.

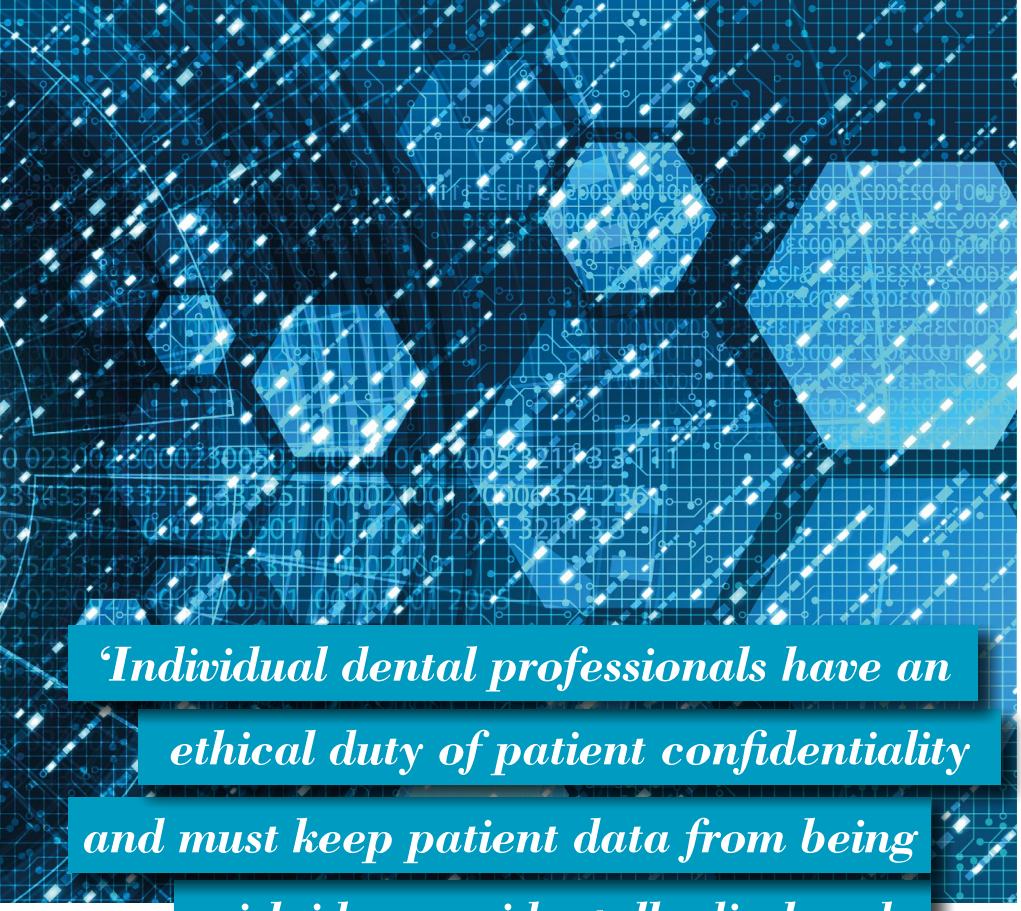
Any data breach or loss of data should be reported to the nominated person within your practice straight away, so that any necessary action can be taken to avoid further breaches and inform patients.

If a data breach is identified, then it may need to be referred to the ICO. To learn whether a data breach meets the threshold for notification, the ICO has developed a self-assessment for data breaches.[5]

All breach notifications need to include the type of personal data breach, including:

- The categories and approximate number of individuals concerned
- Categories and approximate number of personal data records concerned
- Name and contact details of the data protection officer (DPO) or other contact point
- Description of consequences of the breach
- Description of measures taken or proposed to deal with the breach, including measures to mitigate possible adverse effects.

A data breach in Scotland, Wales and Northern Ireland must be reported via the ICO breach reporting tool in each jurisdiction.



'Individual dental professionals have an ethical duty of patient confidentiality and must keep patient data from being mislaid or accidentally disclosed. Failure to do so may result in a patient complaint or even a GDC investigation.'

Case study

Below is a fictional dilemma based on the types of calls we receive on this topic from DDU members.

A member of staff at the dental practice had accidentally given a patient a paper copy of the surgery day list, which included other patients' names, contact details and medical histories.

Unfortunately, the incident above is a GDPR personal data breach, and as such should be treated as an information security incident.

The practice data controller and DPO would need to be informed as soon as possible, as would the patients concerned. The patient should be informed to return the day list to the practice securely, and without delay.

Due to the significant impact on the affected patients, including the potential for confidential medical details to become known to others, it is likely that the practice's DPO would advise to notify the ICO that a data breach had occurred and to this as soon as possible, and no later than 72 hours after becoming aware of the breach.

This situation also highlights the importance of in-house staff training so that lessons could be learned, and to prevent something similar from happening again in the future.

References

1. Intersoft Consulting. Art. 4 GDPR: Definitions. Available at: https://gdpr-info.eu/art-4-gdpr/ (accessed June 2023).
2. ICO. For organisations. Available at: https://ico.org.uk/for-organisations/ (accessed June 2023).
3. General Dental Council. *Standards for the dental team.* September 2013. Available at: https://standards.gdc-uk.org/Assets/pdf/Standards%20for%20the%20Dental%20Team.pdf (accessed June 2023).
4. NHS Digital. Protecting patient data. 14 November 2022. Available at: https://digital.nhs.uk/services/national-data-opt-out/understanding-the-national-data-opt-out/protecting-patient-data (accessed June 2023).
5. ICO. Self-assessment for data breaches. Available at: https://ico.org.uk/for-organisations/report-a-breach/personal-data-breach-assessment/ (accessed June 2023).

https://doi.org/10.1038/s41407-023-1917-z