Data security: How not to become the next Ashley Madison

By Naz Haque, UK

At the heart of the relationship between a dentist and a patient lies trust and respect. Unless you have been hiding under a rock, I am sure you have heard of the Data Protection Act (DPA) 1998 and patient confidentiality, both of which exist to support these relationships. Recent events, such as the Sony or, more currently, the Ashley Madison breach, have brought to public awareness the importance of securing one’s data.

Data security and governance is a very tricky area. I must make it clear I am not a lawyer, and practices should make their own decisions about specific aspects of Care Quality Commission (CQC) compliance. I am a highly experienced information technology professional with a good understanding of data protection and other relevant legislation. All interpretations provided here are my own.

Even if a dental practice has not embraced the digital age and all records and correspondence are in paper and based, the practice still has a number of responsibilities regarding data security. As dental practices collect patient details, they must register with the Information Commissioner’s Office (ICO). Dental records must be stored safely and securely for a number of years (up to six years for the National Health Service; NHS) and kept for a maximum of 30 years (Department of Health).

Aside from the General Dental Council, NHS and CQC governing bodies in the UK, there are a number of legislative acts, the DPA being the most well known, that require dental record storage, such as the Consumer Protection Act 1987, under which an action could arise for a defective product (such as implants), the Medical Devices Directive (Council Directive 93/42/EEC), which relates to custom-made devices (such as retainers or aligners), as well as the Medicines Act 1968 and the Misuse of Drugs Regulations 2001. Records must also be disposed of in a policed manner to avoid fines.

What about dental practices who have embraced digital? Data is accessed in two situations, storage and movement. If you are using one of the popular industry online compliance and provide guidance on keeping up-to-date and resolving these issues. Make sure your data is secured and protected before it is too late.

The next area of concern then is movement of data. This can be via e-mail online referral to or correspondence feedback platforms or devices, and your website. E-mail is not a secure medium, and communication with patients about their medical history or medical circumstances using this platform raises potential issues. The service provider you use for your e-mail could also be inadvertently making you breach data security rules. For example, if you are using one of the popular US-based organisations for e-mail, such as AOL, Hotmail and Gmail, and liaise with your patients via this e-mail platform, you have to consider where the e-mails are being stored, most likely on servers outside the UK.

The DPA states that “personal data shall not be transferred to a country or territory outside the EEA [European Economic Area] unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.” As a dental practice, you should reconsider if you are using a commercial e-mail provider to liaise with your patients, and determine whether your website communication tools and feedback portals are compliant and if not ensure your designated data policy controller addresses this as a priority.

The ICO can issue monetary penalty notices, requiring organisations to pay up to £500,000 for serious breaches of the DPA occurring on or after 6 April 2010. If you have reservations, there are a number of solutions to protect practices from these risks. Clients at Dental Focus expect us to take care of online compliance and provide...