Data security: How not to become the next Ashley Madison

At the heart of the relationship between a dentist and a patient lies trust and respect. 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, but 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 ink and paper 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) here in the UK. 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). 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, the same as physical records are. This also means that there are the two situations in which data can be compromised in the digital world. Dental practices have an obligation to ensure patient data is backed up, recoverable (in case of disasters), secure and protected. This applies during both storage and movement. If you are using one of the popular industry patient management systems, such as EXACT (Software of Excellence), it should have features to support this in place; liaise with your account manager to verify this.

The next area of concern then is movement of data. This can be via e-mail, online referral tools or portals, 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 your own country.

The UK’s Data Protection Act 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. Here in the UK, 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. Clients at Dental Focus expect us to take care of 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.

_Naz Haque, aka „The Scientist“, is Operations Manager at Dental Focus. He has a background in mobile and network computing, and has experience supporting a wide range of blue-chip brands, from Apple to Xerox. As an expert in search engine optimisation, Naz is passionate about helping clients develop strategies to enhance their brand and increase the return on investment from their dental practice websites. He can be contacted at naz@dentalfocus.com._