OPINION

Nigel Knott

DOI: 10.1308/rcsfdj.2019.10

The protection of sensitive patient data online

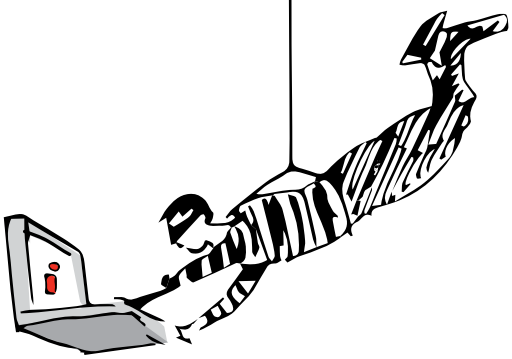
by Nigel Knott

The problem with the threat of cybercrime is a belief that it only happens to others… unless, of course, you are one of the 380,000 British Airways (BA) customers who received an email informing you nearly one week (or more) after the event that your personal data and bank card details had been hacked!

Author: *Nigel Knott, Dental Surgeon and CEO of Dentsure Ltd, 6 Union Road, Chippenham, Wiltshire SN15 1HW*

E: *njk@dentsure.co.uk*

Keywords: *Data protection, patient data*



The BA email message sent to the affected customers said:

The personal information compromised includes full name, billing address, email address and payment card information. This includes your card number, expiry date and CVV. Unfortunately this information could be used to conduct fraudulent transactions using your account. We recommend that you contact your bank or card provider immediately and follow their advice.

British Airways have taken steps to prevent any further data theft, the website is working normally, and we are working with the authorities to investigate how this theft occurred.

This cybercrime first came to my attention via the BBC News website early one morning and despite the BA statement that all customers had been informed, this was not the case. How did the cybercrime theft that began on 21 August 2018 continue for the best part of two weeks (and possibly longer) without discovery?

Next began the frantic rush to contact the bank followed by a delay of nearly one hour before the telephone was answered! And guess what advice was given eventually? 'There is no need to worry as our firewalls and data security are extremely reliable, and there is no need to cancel your bank card.' (Name of the bank supplied on request.) All this in the face of the latest news from UK finance that £360 million has disappeared from customer bank accounts as a result of cybercrime in the first half of 2018.

We know in dentistry from long experience that prevention is better than cure and the same should apply with online/offline data security. The loss of cash is one thing but clinical records and sensitive personal data are a different ball game altogether, and are all too easily brushed off as being a rather trivial matter, as in the case of BA.

The fact that this particular incident has resulted in sensitive personal data ending up in the hands of data brokers operating within the dark web and eventually being converted into cash is being completely ignored by BA. What do they propose to do about it apart from compensating for actual financial loss? They say their website is 'operating normally' but offer no information on how the crime has been remedied. Did the Information Commissioner's Office (ICO) send in a team of IT specialist hackers immediately afterwards to carry out penetration testing of the website in order to confirm it is functioning 'normally'? Are the BA back office systems and privacy notice measures fully compliant with the General Data Protection Regulation (GDPR) and Privacy and Electronic Communications Regulation (PECR) in practice? Has the data protection officer been fired? I doubt it.

But one thing is obvious: much tighter regulation is necessary, and I believe a method of certification/accreditation for company/practice information and communications technology (ICT) systems and online services is long overdue. The acres of print relating to Data Protection Act compliance demand highly specialised IT knowledge and being ahead of what has become an extremely sophisticated area of criminal activity is quite a challenge.

In my article concerning the GDPR in the April 2018 *FDJ*, I stressed the need for all dental practice principals to hone their IT knowledge and skills in order to ensure their practices were fit for ICT usage.[1] A recent personal study of dental practice websites and their practice privacy notices discloses an alarmingly high number of practices that are not GDPR/PECR compliant. The most common breaches concern insecure data harvesting templates (Patient Referrals, Contact Us, New Patient Registration, Feedback, etc) and uncertified email services that fail to include fully encrypted return pathway messaging for patients. This suggests that the field of regulation is not being monitored too efficiently. Is it the ICO, the General Dental Council or perhaps even the Care Quality Commission who may be culpable? Guidance on the reporting of patient data losses and cybercrime can be obtained from the ICO website.[2]

Data protection has moved up the list of priorities in the world of statutory regulation inasmuch as the financial penalties have been increased dramatically. However, this financial deterrent may still not be enough as is evidenced by the frequent breaches of the Data Protection Act. The latest figure of around 50 million Facebook users' data being compromised is truly staggering. Indeed, the last Information Commissioner believed that a jail sentence would be required to bring to book those still operating with gay abandon in what is widely known as the Wild West of the internet.

Data protection has moved up the list of priorities in the world of statutory regulation inasmuch as the financial penalties have been increased dramatically

I have to say that when we compare the criminal act of failing to license a property with a television set receiving live BBC broadcasts with the complete absence of any licensing of premises using potentially dangerous electronic communications, something is rotten in the state of Denmark! I am very familiar with the legislative hurdles that have to be jumped in order to obtain permission to tap into a private telephone line; today the task is a relatively easy one, and rarely discovered with the advent of wireless networks and mobile phones.

Practice websites

A dental practice website is the online equivalent of a shop window. As an experienced dental practice website visitor, I can form a very good idea of the nature and quality of the dental services that the practice provides, and whether it is GDPR compliant. There are often telltale signs of breaches of data protection law so why do the 'authorities' not take any action?

ICT is incredibly complex, and I suspect the majority of the brightest and most highly paid 'geeks' are to be found in the online gambling and pornography markets. My conclusion is that the 'authorities' are well behind the action in the ICT world and lack the necessary resources to monitor the market place sufficiently as they are constantly firefighting. Clearly, some of the bigger fish (such as BA and Facebook) will take up chunks of scarce ICO resources but why are the General Dental Council and Care Quality Commission not doing more to ensure the confidentiality of patient e-records?

The GDPR makes it clear that the regulated professions (such as dentistry) are classified as 'special category' occupations in the field of data protection. The PECR requires dental practice websites to take particular precautions for the online protection of sensitive patient data using electronic communications networks. It is no longer sufficient to publish a practice privacy notice, often populated with far too much small print and hidden away from obvious attention.

We are all guilty of agreeing to small print terms and conditions of website use without actually reading them or understanding the implications of the 'deal' that exchanges precious sensitive data for free use of a service. What is not so well known is a new mandatory requirement to prove the provision of special online security measures in the form of a 'just-in-time' website message (Figure 1). This message must inform website visitors how sensitive personal data entered on any interactive website template (Patient Referrals, Contact Us, New Patient Registration, Feedback, etc) are encrypted before transmission.

Figure 1 Example of a 'just-in-time' website security message

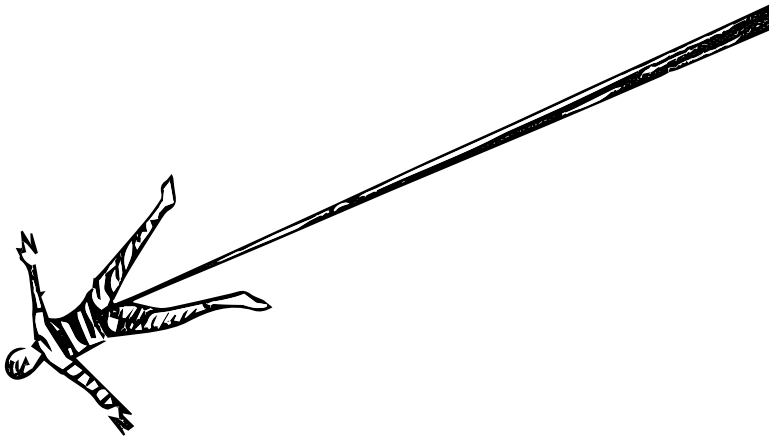
I would hope that practice principals will by now have understood the need to have strict controls in place for the protection of the sensitive patient data they hold in trust on behalf of the owners – the patients themselves. Unfortunately, I am not at all sure they understand the implications of what happens when sensitive patient data are entered in an interactive online website template and then transported electronically to a data centre storage facility (server), wherever that might be.

Most dental practice websites now display a padlock in the address bar, which indicates the existence of a Secure Socket Layer (SSL) certificate. By clicking on the padlock icon, you can determine the nature and validity of this certification. This SSL or Transport Layer Security protocol employs software that encrypts messages sent from the website to a data domain either within or without the dental practice itself.

These certificates come in two forms: either with domain validation (DV) or with extended validation (EV) identity. A DV certificate confirms details of the registered domain address of the website while an EV certificate is only issued once the dental practice principal has provided documentary proof of domain ownership to the certificate provider. EV certification informs website visitors that this is an accredited dental practice website where messages sent to the server are fully encrypted, but it does not tell you what happens to the data once they arrive within a remote data server outside the confines of the practice itself. So while the website might be properly published and authenticated on the internet, are the email address hyperlinks safe to use and the interactive message template communications securely connected to a certificated server with the data remaining encrypted? In the absence of a GDPR-compliant just-in-time notice, the answer has to be 'no'.

Data security certification

Having dealt with the e-communications pathways from the website to the secure data centre or server, where the data is *not* stored in plain text, we need to establish whether the server itself is in or outside the EU safe harbour area and whether it carries some form of security classification (eg the ISO 27000 series on information security). Dental practice data controllers would be well advised to choose UK-based internet service providers (ISPs) with proof of ISO 27001 accreditation. ISO 27001 requires a standard information security management system (ISMS) to be in place. The ISMS is a framework of policies and procedures that include all legal, physical and technical controls involved in an organisation's information risk management processes. I am an advocate of the use of ISO certificated ISPs whenever possible.



All ISPs and software providers should be made the subject of a written contract that is properly documented. It is not sufficient for an ISP to state their services comply with the GDPR/PECR; the documentary evidence should state clearly what security measures are in place to protect all sensitive data within their care from being accessed by unauthorised third parties. Practice management software systems should also have written contracts containing online security protection certification.

Whilst I believe that the ICO should introduce some form of data security certification for the special category professions in the long term, data controllers in the short term must document all patient data processing protocols (including those of *all* data processors) and ensure data transfers made from the firewalled central practice database are properly securitised and their destinations recorded. Dental practice principals should be well aware by now that the 'no free lunch' saying applies in spades in the online world of the internet.

Specialist referral practices

Some practices quite rightly prefer to play safe and provide website patient referral templates employing a secure offline 'print and send' facility. Others, however, fall far short of what is required for the security of online patient referrals. Referral practices have a special duty of care as they are responsible for the protection of all patient data being transferred online from referring practices. Referring practices are entitled to know exactly what special precautions have been taken online in advance of sharing and transferring sensitive patient data that may include a medical history. In these instances, a website just-in-time message is mandatory (see Figure 1) in order to comply with the GDPR. Online referral practices must satisfy their referring practices that it is safe to refer their patients via their practice website. A properly certificated interactive website facility with encrypted referral forms will save time and money by introducing much greater efficiency. The compliance benefits for your practice are discussed in the ICO publication, *The Privacy Dividend*.[3]

Conclusions

Big data today are worth big bucks and while it is true that cybercrime attacks are being directed increasingly at the lucrative big organisations, there are many areas where data are aggregated from a collection of small specialist organisations. Nobody can be considered immune from cybercrime and the healthcare sector is an attractive environment from which third parties can harvest very valuable personal data. Practice management system software, practice backup facilities, insecure emails and frequent online data transfers via practice websites are all particularly vulnerable areas of concern.

Ensure your firewalled patient database is accurate, up-to-date and of fortress status. Whenever any data are transferred/shared, they should enjoy armour-plated protection. Never forget that acting in the best interests of your patients includes the protection of their confidentiality.

23 October 2018

Postscript

Since this article was first submitted for publication, further evidence has emerged in respect of the BA personal data hacking incident. On 25 October 2018, BA disclosed that another 185,000 customers' personal data from bookings made online between 21 April and 28 July 2018 were compromised. Surely the ICO should be making a public statement confirming it is now safe to entrust BA with our personal data? The least we can expect is verification that BA's ICT systems have been investigated by a team of software specialists appointed by the ICO to ensure the company complies in every detail with the GDPR and the PECR.

Self-certification of personal data protection has manifestly failed at BA, and until confidence and trust has been restored by a reliable third-party audit, I for one will not be using BA's online booking facilities. Following another recent data breach at Heathrow Airport Ltd, it was revealed that only 2% of the 6,500 employees had received any formal training in data protection. *Caveat emptor.*

1 November 2018.

Reference

1. Knott N. The General Data Protection Regulation. *FDJ* 2018; **9:** 54–57.
2. Information Commissioner's Office. *Report a breach.* https://ico.org.uk/for-organisations/report-a-breach/ (cited November 2018).
3. Information Commissioner's Office. *The Privacy Dividend.* Wilmslow, UK: ICO; 2010.