# Website warning

**Nigel Knott** reviews the developments in internet security.

More than two years ago I published several articles in The Dentist concerning dental practice websites. It should have been fairly obvious to even the most computer illiterate of those who read these articles that there was a regulatory time bomb of non-compliance waiting to detonate.

Since then, the bomb has acquired nuclear potential and it is still ticking. When it will explode is anyone's guess but my forecast is fairly soon, with the GDC/CQC and the Information Commissioner's Office (ICO) all generating smoke signals it would be foolish to ignore.

All GDC registered personnel will have received a new set of professional standards. Principle 4 of the new GDC Standards is devoted entirely to patient confidentiality and the need to use encryption technology when sending emails. This however represents only half of the story. The ICO Booklet A Practical Guide to IT Security gives more explicit advice for small businesses, "keeping an IT network safe and secure can be a complex task and does require time, resource and specialist knowledge". I can say from long experience that understanding all of the implications for dental practices can be a daunting task. In the days when computers were used solely for practice administration and management, things were relatively simple. Today the telephone wires carry data in and out of the practice via a broadband connection and so the problems begin.

**Nigel Knott**
is a dentist and CEO of Dentsure.

**Problems**

There is a dangerous complacency within some dental practices where the Data Protection Act is considered to be not terribly important. It is the online dimension that is so risky and this is not surprising when you consider all of the dangers that lurk in the world of the internet and wireless communications. The news headlines are packed with stories about the loss of sensitive personal data and how easy it is for the data hackers to operate within unprotected electronic networks. Indeed Yahoo, Hotmail and Google make no bones about the fact that they harvest personal data for commercial purposes. No secrets there then and no free lunch either.

Any dental professional who has not made the necessary arrangements for the protection of sensitive patient data being transferred or shared online without proper security in place is breaking the law. Data Protection principle 7 is the one that everyone has to obey: "Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data."

I have had a dentist send me an e-mail recently which said, "So what, nobody cares." In other words, "I am breaking the law and nobody cares so why worry?" This is bizarre. Another dentist has had a Yahoo account hacked and a number of patients have been approached for money to be sent to pay for a return to the UK from a post-graduate conference in Manila. The message informs patients that personal belongings have been stolen including passport, air tickets, credit cards and cash with pleas to deposit a sum of money to be paid into a bank account within 48 hours to pay for the return home.

In another recent case involving the loss of patient personal data, an enforcement order (ENF0466943) was served by the ICO on a medical practice using insecure email facilities for patient contacts.

These problems are compounded by the fact that there are a number of web agencies/internet service providers (ISPs) that see a fast buck in dentistry and practice principals are placing far too much reliance on flawed advice and unsafe services. All of the regulated professions have special responsibilities and outside web agencies are frequently unaware of the onerous additional regulatory responsibilities. Think of the damage and inconvenience to➲

your practice if you lose your website presence, your e-messaging facility or even your internet connection.

What baffles me is the fact that there are no healthcare industry standards in place as an example of what needs to be done for the protection of sensitive patient data transfers online. The payment card industry issues very detailed measures that must be made for consumer protection and these are confirmed by the routine presence of padlocked green bar/https:// website address access codes. I have first hand experience of website agencies/ISPs operating in the dental field which are breaking the law. Some are not even registered with the ICO and the same comment applies to about 10 per cent of dental practices.

Dental practice websites are becoming the subject of much greater scrutiny as there are so many regulatory issues that range from advertising standards, website security, e-messaging security and a raft of GDC regulatory requirements. Have you ever analysed the risks not only of having sensitive patient data going astray arising from a criminal act but also the dangers of your web agency breaking the law as well?

How many web agencies/ISP's operating in the dental field are made the subject of a legally binding contractual agreement set down in writing with very clear duties and responsibilities? Do you actually know what the status of your website is? What happens if you lose your hosting services or worse still your Uniform Resource Locator (URL or web address) and what redress do you have? Are patient data transfers (particularly specialist referrals) from your website the subject of secure encryption arrangements? These are questions you will need to answer with certainty as part of a Privacy Impact Assessment (PIA) that should be carried out at regular intervals.

It is my personal belief that before long the GDC annual registration fee will include a requirement to supply proof of ICO registration and CQC accreditation. The NHS has made it clear that no new dental contracts will be awarded to any practice without the basic ICT ingredients of the NHS Information Governance Toolkit being in place.

The task for every dental practice principal is made even more difficult by the fact that watertight advice to help resolve the all too obvious IT risks is scarce. Expecting every GDC registrant to comply with all of the requirements of the Data Protection Act in the absence of any reliable professional advice (or funding) is unreasonable.

**IT challenges**

Let's start in the beginning with the ICO Notification (registration) process and the declaration of purposes.

It is good practice to name personally your data controller (this is much better than using your practice title) and publish on your website your ICO registration details with a link to the ICO register (**www.ico.org.uk/ESDWebPages/DoSearch**) where any third party can check the veracity of the information you have provided. Patients expect your professional registration details and qualifications to be readily accessible on your website (GDC requirements) and so should details of your patient data protection arrangements. My recommendation is to publish a practice privacy policy that includes all of this information on a separate web page

with a link from your home page.

All data controllers must declare that data transfers are all made within the EEA and subject to common data privacy laws.

Do you know where patient data are stored/processed/backed up from your practice database or your website? Is your email securely encrypted? Does your website have online referral facilities providing the necessary DPA compliance for referring practice data controllers? Are the website templates properly secured and the data transfer pathways known? Do you have a written data sharing agreement in place?

Your practice privacy policy must include a very clear statement about electronic tracking devices such as 'cookies'.

Here again your web agency/ISP must be made the subject of very clear instructions about any cookie requirements being strictly necessary for specific professional purposes. Many cookie users embrace them for purely commercial reasons and the practice is particularly common in the worlds of online betting and pornography in order to keep in regular touch with website visitors. The gratuitous and unnecessary use of cookies is an undesirable threat to personal privacy and hence the need for regulatory controls.

**Solutions**

Here is some practical advice:

- Use strong passwords which are case sensitive.
- Do not store personal data, especially personal health information on your website.
- Carefully monitor the website logs to make sure that any changes to your website are lawful.
- Make sure that you are aware of web agency/ISP security precautions and the location and status of their hosting facilities (EEA).
- Use internet experts to test your website security.

Email messages can be read like a post card and the only safe method of protecting sensitive personal data is to ensure it is encrypted at all times between data being entered on a website template and being transferred to and deciphered by a named data controller. Your web site hosting facility should be used to provide a properly hosted safe data exchange depot.

- Proprietary email is insecure and unsuitable for professional purposes.
- Provide a secure website template for patients/dentists to contact the practice.
- Obtain the informed consent of every patient if you wish to use email.
- Email addresses must be correct and sensitive patient data should not be included in your e-messages.
- Label all email messages as private and confidential.
- Publish a practice privacy policy on your website.

**Conclusion**

This is all rather dry and serious stuff. However my warning is designed to bring to the attention of all practice principals the dangers of publishing dental practice websites on the internet that fail to comply with the complex raft of ICO/GDC/CQC regulations. The information commissioner has stated publicly he is not content with his present powers to impose a fine of up to £500k and he is seeking to increase them to include jail. You have been warned.