The use of information and communications technology (ICT) in dentistry

N. J. Knott[1]

IN BRIEF

- Identifies widespread problems associated with breaches of electronic commerce laws.
- Lists a number of precautions to help practice principals understand their professional responsibilities and how to protect patient information.
- Suggests the GDC should introduce a compulsory verifiable CPD module – the use of ICT as part of the new professional standards guidelines.

OPINION

As the use of information and communication technology (ICT) becomes more widespread in dentistry the risk of breaching electronic commerce laws and patient confidentiality increases. It is necessary to be aware of the responsibilities internet usage entails, especially within a dental practice where the protection of patient information is of the utmost importance. More should be done to outline the various precautions that should be taken to ensure ICT security within the professional domain, as it would appear dentistry has been a neglected industry with regard to receiving the proper ICT education, training and support system.

SUMMARY

As so often happens within the spectrum of primary healthcare, dentistry is treated as the poor relation – it is the Cinderella of medicine. Nowhere is this more apparent today than in the field of ICT. Not only have general medical practitioners (GMPs) enjoyed massive taxpayer subsidies to provide them with the necessary education and training in the use of ICT but also the accompanying hardware, software and an exclusive secure electronic communication network (NHS Net). Dentistry therefore is left in a state of detached anarchy in the hands of unregulated internet service providers (ISPs) and software engineers. No electronic 'look and book' facilities to make a GDPs life easier for patient referrals to NHS Hospital facilities but the good old fashioned use of pen and paper delivered by the Royal Mail must remain the order of the day! The specially designed NHS mechanism to deliver futuristic personal dental services (PDS) – the Primary Care Trusts or PCTs – has been disbanded and an integrated IT strategy for dentistry is as far away as ever, archived somewhere within the Department of Health plans for the long awaited new NHS dental contracts!

At the beginning of the new millennium the Government published a number of grandly named strategies under the umbrella policy of an e-government interoperability network in response to the EU directive on electronic commerce.[1] Soon afterwards the Information Policy Unit of the NHS issued a *Strategy for cryptographic support services in the NHS*[2] about the time the NHS secure communications network service 'NHS Net' was rolled out by BT, cable and wireless. In another major policy document *Shifting the balance of power: the next steps*[3] dentistry gets a mention under the provision of personal dental services (PDS).

In October 2002 *An IT strategy for dentistry in the 21st century* arrived from the Department of Health.[4] This document included the following proposals:

- The overriding theme is the reintegration of dentistry within the NHS and for dental records to become more connected with mainstream NHS IT
- Electronic patient records including digitised radiographs will need to be transferable between dentists and other organisations
- To achieve this vision there will need to be a substantial investment in education, training and change management for dental practices
- A programme manager has been appointed to carry out the preparatory work needed to implement the dental IT strategy.

Dentistry is no nearer to being provided with a solution to the ICT problems facing it today than when this strategy was launched more than a decade ago. No doubt the programme manager – whoever might have been recruited to the post at the time – has now been pensioned off with a lump sum bonus for failure!

THE PROBLEMS

While definitive data on the subject of the use of ICT in dentistry are difficult to obtain, there are two *BDJ* articles[5,6] reviewing the publication of dental practice web sites and a BDJ/BDA/Nature Publishing Group (NPG) survey[7] that deals with the dentists' use of ICT. While only a little light is shed on the ICT situation in general dental practice the nature of the difficulties are obvious – there is a systemic problem associated with widespread breaches of the Professional Regulations and Data Protection Act 1998 where the use of ICT in dentistry is concerned. It is a classic case of the tail wagging the dog.

The first *BDJ* article published in 2005 *Does your practice website need updating?*[5] discloses the fact that no dental practices surveyed were compliant with the EU regulations on web advertising, while the second published in 2011 *Quality and content*

[1]CEO Dentsure Ltd, 6 Union Road, Chippenham, Wiltshire, SN15 1HW
Correspondence to: Nigel J. Knott
Email: njk@dentsure.co.uk

Accepted 19 December 2012
DOI: 10.1038/sj.bdj.XXX

of dental practice websites[6] confirms the fact that very few dental practice websites conform to all of the relevant regulations that apply to website content and secure e-communications (e-mail). The BDJ/BDA/NPG ICT survey[7] is more broadly based but unfortunately it does not give us a very clear picture of what is going on in general practice where the use of ICT is concerned. Of 2,806 BDA members who were approached in the survey only 500 eventually took part and of these 20% were full time salaried NHS staff. However, the results suggest that less than 50% of UK dental practices have websites and a very large proportion of dentists rely on free insecure proprietary internet communications for professional purposes. It is likely that many of those who did not take part in the survey were discouraged by the fact they were not familiar with the use of ICT or did not have any computerised functions within their practices. It is known also that a significant number of practice principals are neither ICT literate nor have any intention of becoming so in the near future as the magnitude of the task and the costs are major deterrents. This is despite the fact that no new NHS dental contracts will be given to dental practices that are not fully computerised and compliant with the NHS Information Governance Toolkit.[8] Presently, the widespread regulatory non-compliance is very likely the result of practice principals being unfamiliar with the details of the Data Protection Act 1998, regulations concerning the use of electronic communications, and website agencies being unaware of the GDC professional regulations concerning the special security required for the protection of patient identifiable information (PII). This potent combination leads to the existence of a systemic risk of non-compliance and the potential threat to a practice principal of a maximum fine from the Information Commissioner's Office of £500,000 accompanied by GDC disciplinary proceedings and professional sanctions. The Leveson Inquiry and ever increasing cyber crime activity should be enough to galvanise the dental profession into taking meaningful preventive measures sooner rather than later.

With the advent of computer assisted design (CAD) and computer assisted manufacturing (CAM) technology the problems will become more acute as prosthodontics will depend very much upon CAD/CAM-based technology. In future, clinical treatment planning might be prejudiced without the knowledge and application of the very latest computerised solutions (CAD/CAM).

IMMEDIATE PRECAUTIONS

1. Although the NHS Information Governance Toolkit[8] takes some assimilating, it is nothing more or less than a statement of good governance where the use of computers and ICT in dental practice is concerned
2. The Information Commissioner's Office also publishes some excellent booklets all of which are available online giving clear guidelines that have to be implemented to comply with the Data Protection Act 1998 (www.ico.gov.uk)
3. A named data protection officer (preferably a practice principal or the practice manager) and data controller should be in every dental practice and registered with the ICO under the Data Protection Act 1998
4. All appointed data controllers should study the ICO *Data sharing code of practice*[9] in detail and carry out a privacy impact assessment (PIA) as a matter of urgency. There should be written contracts in place with internet service providers and web agencies placing the onus of responsibility upon their shoulders for Data Protection Act compliance. All e-communication networks need to be secured for the transfer of PII and hosting arrangements must comply with the ICO notification guidelines[10]
5. Ensure your dental practice URL (uniform resource locator or web address) is registered in the practice ownership and ensure the IP (internet protocol) address is properly authorised and the hosting facility compliant with the professional regulations where PII transfers are concerned
6. Validate the status of your e-mail service and ensure that your professional e-communications facilities are fit for professional purposes and separated from personal facilities
7. Websites should be categorised into either static information only (no e-communication hyperlinks) or active (secure e-communications and compliant hyperlinks). The practice of harvesting sensitive patient data (PII) through insecure website templates is asking for serious trouble. There should be no web site e-communications (referrals/appointments/new patients/ contact us/ e-mail addresses) in the absence of secure transmission pathways (https://protocols) and secure socket layer (SSL) protection to and from secure hosting facilities. Patient identifiable information (PII) must be fully encrypted so it cannot be intercepted by anyone other than a certificated data controller. **No PII (e-data) should ever be stored within remote hosting facilities (servers) in plain text where it can be read by a third party.** In the case of information only (brochure) web sites there is no objection to print and send (PS) protocols being employed where patient forms are published in a portable document format (PDF) that can be downloaded, completed offline, authenticated and sent by post
8. Regulations must be enforced for any IT/web agency working within dentistry. It is an offence for any agency to use the word 'dental' or 'dentist' (or other protected words associated in meaning to the practice of dentistry) in a company title unless it has been properly authorised and approved by the GDC beforehand. Companies House will not register a particular company title without evidence of certification by the GDC that audit processes designed to protect the profession and their patients have been approved
9. Carry out due diligence on any outside ICT contractor via Companies House and the ICO Public Register. An assessment of specialist knowledge, experience and competence should be made before any outside service contracts are executed.

PROFESSIONAL STANDARDS AND SOLUTIONS

The BDA should be working in concert with the GDC/ICO to ensure educational

facilities are available to address the ICT problems and publish clear professional compliance guidelines as part of the BDA Good Practice Scheme. It would be beneficial for the GDC to introduce ICT as a compulsory verifiable CPD module and integrate this with revised professional standards.

The Government should be compelled to provide postgraduate funding on a national basis in accordance with the *IT strategy for dentistry*.[4] Professional regulations cannot be easily implemented in the absence of clearly stated professional guidelines and properly funded and approved education facilities.

Plans must be published to finance and integrate all primary dental care facilities into the NHS Net virtual private network (VPN) without delay. All patients are entitled to NHS secondary care (hospital) benefits and there is a case therefore to include all UK dental practices offering primary care facilities irrespective of their NHS or private vontract status.

All internet service providers (ISP's) and website agencies should be properly scrutinised and subject to clear contractual arrangements in accordance with the Data Protection Act 1998 and the professional regulations governing electronic commerce in dentistry.

1. Directive 2000/31/EC of the European parliament and of the council. *Official journal of the European Communities, 2000.* Online directive available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:178:0001:0001:EN:PDF (accessed January 2013).
2. Department of Health. Strategy for cryptographic support services in the NHS. London: *NHS Information for Health, 2001.* Online article available at http://webarchive.nationalarchives.gov.uk/+/www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4008681 (accessed January 2013).
3. Department of Health. *Shifting the balance of power: the next steps.* London: DH, 2007. Online article available at http://webarchive.nationalarchives.gov.uk/+/www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/Browsable/DH_4099025 (accessed January 2013).
4. Department of Health. *An information technology strategy for dentistry in the 21st century.* London: DH, 2002. Online article available at http://www.dh.gov.uk/prod_consum_dh/groups/dh_digitalassets/@dh/@en/documents/digitalasset/dh_4058891.pdf (accessed January 2013).
5. Addy L D, Uberoi J, Dubal R K, McAndrew R. Does your practice website need updating? *Br Dent J* 2005; **198:** 259-260.
6. Nichols L C, Hassall D. Quality and content of dental practice websites. *Br Dent J* 2011; **210:** E11.
7. Dentists' ICT use. BDJ/BDA/NPG Survey, October 2011. London: NPG, 2011.
8. Information Governance Training Tool. Online information available at https://www.igte-learning.connectingforhealth.nhs.uk/igte/ (accessed January 2013).
9. Information Commissioner's Office. *Data sharing code of practice.* Wilmslow: ICO, 2011. Online article available at http://www.ico.gov.uk/for_organisations/data_protection/topic_guides/~/media/documents/library/Data_Protection/Detailed_specialist_guides/data_sharing_code_of_practice.ashx (accessed January 2013).
10. Information Commissioner's Office. *A complete guide to notification.* Wilmslow: ICO, 2010. Online article available at http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/notification_handbook_final.pdf (accessed January 2013).