www.independent-practitioner-today.co.uk March 2020 Issue 119 £12.50

INDEPENDENT PRACTITIONER TODAY

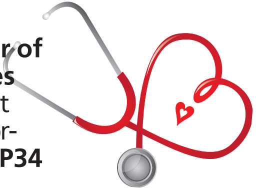
The business journal for doctors in private practice

Eight more pages of coverage begin on page 8

In this issue

Don't let data fall into the wrong hands
We show you how to avoid data handling mistakes **P28**

How to steer clear of amorous advances
When boundaries get crossed in the doctor-patient relationship **P34**



On the same path to retirement?
An adviser reveals the conversations you should be having now **P42**

Top reasons for data breaches

IN THE non-cyber category – that is to say, 'human error' – we have, as the main causes:

- General breach of personal data – this will contain 'blagging' incidents and the accidental disclosure of personal data;
- Data posted or faxed to incorrect recipient;
- Data emailed to incorrect recipient;
- Loss/theft of paperwork or data left in an insecure location.

In the cyber category, we have the following main reasons for data breaches:

- Phishing – emails with malicious links, malware;
- Unauthorised access.

In conclusion, it is errors by staff and employees that cause the majority of data breaches reported to the ICO.

Poor data handling and data management are underlying causes for the data breaches reported to the ICO, whether these breaches are cyber or non-cyber.

Errors in the use of emails is a big factor behind data issues, where we see common problems such as:

1. Emails sent to incorrect recipients.

2. Emails with people pretending to be someone else – 'blagging'.

   Blagging occurs when someone poses as a trusted individual to obtain personal information from their victim or encourage the victim to perform actions, such as a bank transfer.

3. Emails containing phishing and other scams and malware. Phishing is an attack used to steal data including login details and credit card details.

   The attacker will generally pose as a trusted entity and dupe the victim into responding to an email or text message.

4. Emails with incorrect or wrong content and referencing of individuals.

Other common reasons for data breaches are:

- Theft of data or equipment on which data is stored;
- Inappropriate access controls to information systems and paper files, allowing unauthorised use;
- Disclosure of patient or employee data to unauthorised sources;
- Equipment failure;
- Human error – for example, losing paperwork, USB sticks, inadvertently altering data;
- Hacking attack.

How to avoid data breaches

For practices who have invested in well written and practice-specific data handling guidelines, together with regular staff training, data breaches from human errors can arguably become largely avoidable.

> **"It is errors by staff and employees that cause the majority of data breaches reported to the ICO"**

Cause: Breaches via email use

Prevention:

- Staff training and updates;
- Cyber security software tools, regularly updated, which protect against phishing, malware and other email-based attacks;
- Data handling guidelines for attachments, storage of data and data accessed outside of the office;
- Operational procedures to validate identity of individuals.

Cause: Unlawful disclosure of patient or employee data

Prevention:

- Staff training and updates;
- Operational procedures to validate identity of individuals;
- Role-based access controls on all information systems.

Cause: Loss/theft of data in soft or hard copy

Prevention:

- Staff training and updates;
- Data handling guidelines for use of external storage devices such as USB sticks, home computers, phones and other remote devices; in short, all data transfer or access outside the protected office environment;
- Secure data disposal routines.

> **It is crucial that practice owners appoint individuals to be responsible for ongoing staff training, data handling standards and security procedures**

Cause: Inappropriate access to data
Prevention:

- Staff training and updates;
- Role-based access controls on all information systems;
- System auditing and logging.

Cause: Hacking attacks
Prevention:

- Business continuity plans.

Cause: Equipment failure
Prevention:

- System failover (back-up) and recovery practises for key business operational systems; for example, practice management systems.

Staff training

Staff training is crucial to reduce the risk of data breaches. With a majority of the reported data breaches being caused by human error, it is essential that staff are given the knowledge to do their best to prevent these 'accidental' breaches.

Data handling guidelines

Writing simple and easy-to-follow guidelines for all staff can be an effective way for employees to access information on how best standards apply when processing patient data.

It is easy to make these guidelines specific to your individual practice by using everyday examples and providing links to other policies and procedures.

Consider addressing areas such as:

- The safe transfer of data;
- How to check email attachments;
- Whether your practice offers patient portals for secure data access;
- How to check identity of patients or other individuals who request access;
- How to spot spam emails.

Other practical steps which can be taken to help with security of data are:

- Consider locking down USB ports on practice machines so that data cannot be downloaded;
- Secure shredding of data;
- Put in place a theft-reporting procedure
- Regularly check who has access to your systems;
- Ensure data back-ups are regularly undertaken;
- Update cyber security tools regularly.

In summary, there is a lot that practices can do to reduce the risk of data breaches, especially those by staff.

Training of staff is clearly hugely beneficial. It is crucial that practice owners appoint individuals either within the practice or as an outsourced service to be responsible for ongoing staff training, data handling standards and security procedures.

With data breaches, it is commonly said that 'it's not a case of IF, but WHEN'. So, the best approach is to, be prepared.

■ **See 'Guard your systems from cyber attacks', page 36**

Jane Braithwaite (right) is managing director of Designated Medical, which offers business services for private consultants, including medical secretary support, bookkeeping and digital marketing.

Karen Heaton is the founder of Data Protection 4 Business, which offers consultancy services to design and implement GDPR-compliant solutions, as well as online training, outsourced Data Protection Officers and specialised software technology to support data protection compliance.

Together, Designated Medical and Data Protection 4 Business offer consultancy services and support to help private practices and clinics design and embed a data protection compliance culture into their organisations.