Outcomes from visits to general practitioners and primary healthcare providers

V1.0 22/01/2014

Background

The Information Commissioner's Office (ICO) is the regulator responsible for ensuring that organisations comply with the Data Protection Act 1998 (the Act) and also has a remit for promoting good practice in information handling. The Act consists of 8 Principles of good information handling that all organisations processing personal data have to comply with.

In 2013/14 we undertook 24 advisory visits at GP surgeries across England in order to get a better understanding of the processing they undertake and the circumstances that they operate in. This was in response to requests directly from surgeries and also working with a Clinical Commissioning Group (CCG) and a Practice Manager's forum. We have also conducted audits with out of hours primary care providers.

Whilst this only constitutes a tiny fraction of the number of primary healthcare providers in the UK there were a number of common themes and challenges faced in managing information.

Advisory visits are a one day informal visit to look at how an organisation handles personal information where we provide practical advice and guidance on site and a short report after the visit. The visits typically cover information security and records management and were mindful of the requirements of the Health and Social Care Information Centre's Information Governance Toolkit to General Practice.

This report highlights our experience of personal data handling by GP's surgeries and is intended to help other GPs and Practice Managers see where they can make improvements in how they handle their staff and patient information.

About GP surgeries

GP surgeries are independent contractors consisting of partners and directly employed general practitioners. Most are overseen by a group of partners, and all have a relationship to their local CCG who have a role supporting quality improvement in general practice.

The visits helped to highlight the pressures faced by GPs as data controllers for their patient records in a time of massive change to the structure and practices within the NHS and the corresponding information flows.

In particular GPs have ongoing responsibility for ensuring that there are appropriate contracts in place with all third parties who process patient data on their behalf that covers the security of that data. Historically many of those arrangements were set up and managed by Primary Care Trusts (PCTs) who no longer exist.

The proposed roll out of Care.data in 2014 means that GPs will have to be especially mindful of the need to make their patients aware of how and

why their information will be shared with the Health and Social Care Information Centre and the option for them to object to that sharing.

Typical processing of personal data in Primary Healthcare

Aside from the requirements of the Act to secure information and limit its use and disclosure, a duty of confidence exists and is integral to the trusted relationship between GPs and patients.

The surgeries visited varied considerably in terms of their size, structure, nature of their buildings and also the sophistication of their systems and information processing. However, the surgeries had many shared themes because of the common nature of work they undertake within the NHS.

Surgeries processed the information of their patients and staff members in paper and electronic form. This included patient contact details, date of birth, NHS number and medical records that contain sensitive personal data concerning their physical and mental wellbeing and their treatment going back many years. GPs are the data controllers for this information and it is their responsibility to comply with the Act for records held in their surgeries and handled by contractors.

Patient identifiable information was processed in electronic form in various proprietary patient information systems. This was held either on networked PCs, on-site servers or off site by service providers. Some or all of this electronic information was also duplicated in paper form.

Basic hardware, software and support for both was provided to surgeries, usually under arrangements with PCTs, which have now been replaced by CCGs. The move from PCTs to CCGs has caused some uncertainty across a number of areas, but this was especially apparent in IT and in Information Governance, where some PCTs had previously taken a lead role in supporting and coordinating activity. The surgeries visited were aware of the risks of a discontinuity in approach by CCGs.

There was a paper patient record element for all surgeries visited, although in some cases this had been minimised, but the challenges that 'Lloyd George' envelope filing placed on space, administrative time, and records security were repeatedly demonstrated in all types of surgery.

Areas of good practice

✓ In most surgeries overall responsibility for data protection and Information Governance (IG) was assigned to a specific owner, usually the Practice Manager, and in some cases to a nominated partner or Caldicott Guardian.

✓ Surgeries had version-controlled IG, confidentiality and data protection policies. Policies were frequently owned by the Practice Manager, signed off at a senior level and regularly reviewed. In some cases policies did not state a named owner or review date, and in others had exceeded their review cycles. Although it is not always the case, policies, procedures and protocols were usually easily accessed by staff on shared drives or as hard copies.

Case study – Keep it simple

At one practice visited, a staff handbook had been created, which incorporated information governance and confidentiality requirements, helping to raise staff awareness of their responsibilities.

The Information Governance Policy incorporated simple DO's and DONT's guides throughout each section.

✓ Many surgeries incorporated IG and confidentiality requirements into employment contracts and terms and conditions of employment. They were also included in staff handbooks, helping to raise staff awareness of their responsibilities.

✓ Surgery staff generally showed a good awareness of IG and security issues. Reception staff were usually sensitive to disclosing patients' names when dealing with telephone queries in the reception area, or disclosing to family members without consent. In some cases surgeries are able to provide private areas for discussions with patients away from reception/waiting spaces.

✓ The induction training that staff received when joining surgeries usually covered patient confidentiality, data protection and information security. However, the depth of any refresher training varied between surgeries. Some ensured staff training and awareness remained high with annual e-learning or classroom training. Local groups of surgeries and CCGs had a role to play with some pooling resources to provide IG training and others setting standards to ensure consistent IG awareness.

Case study - A thorough approach to training.

One surgery supplemented e-learning on information governance for all staff with face to face sessions. Training was provided at induction and also regularly refreshed. Locums, temporary staff, students and directly employed cleaners, have equivalent training and a specific locum information pack includes detailed guidance.

The surgery reviewed which online NHS training sessions were appropriate for staff. Training was logged and monitored to ensure that everybody was aware of their responsibilities.

A helping hand.

We have a range of informative and useful free resources which can support your mandatory training or help you to deliver refresher training and/or raise awareness in an interesting and efficient way.

You can watch all of our data protection and freedom of information films on our YouTube channel or on our Vimeo channel. Some of our popular training videos have accompanying scripts and viewer notes.

✓ All surgeries visited showed a strong awareness of the need to dispose of confidential paper waste securely. Specialist contractors were often used, in some cases on group/regional contracts, and provided certificates of destruction. Some surgeries relied on in-house shredding which was sometimes but not always a proportionate response to the volume of confidential waste involved.

✓ Where surgeries had remote working this was usually tightly controlled and appropriately secure dual factor authenticating controls was used.

✓ In general, the surgeries showed a good awareness of the risk of unsecured USB sticks. In most surgeries no laptops or USB sticks were used by any staff. In others, where USB sticks were used these were encrypted.

✓ At most surgeries staff used NHS smartcards provided by their CCG to access NHS Spine data, with staff signing smartcard usage agreements. At most surgeries visited if a member of staff leaves their access to systems is blocked, but some surgeries Access Control Lists contained ex-staff members listed as 'Active' users. Processes for managing this, and maternity and long-term leave, varied in their effectiveness.

✓ Surgeries had different arrangements for staff and their families being patients, with most having rules in place to ensure staff members were registered at other surgeries so that their health records could not be viewed or accessed by colleagues.

✓ In most cases internal doors had digital keypads or locks to support security zoning of different areas of the building, including areas where medical records are held, although in some cases these were not used and doors were left open. Keys were usually kept in lockable key cupboards.

Areas for improvement

! Some surgeries were aware of the need to self-report data breaches to the ICO via the Connecting for Health (now Health & Social Care Information Centre) portal. Procedures were always in place to log serious and untoward incidents, but IG incidents were rarely distinguished. It is only through the thorough reporting of incidents that regulators can properly support organisations encountering incidents and help avoid repeats. As such, failure to report a breach is one of the factors taken in to consideration by the ICO when assessing monetary penalties.

! Where surgeries used CCTV cameras for security purposes, fair processing notices were not always used, and in some cases there was no policy in place regarding how the systems were operated or who had access to the images they created. Where CCTV was operated by a third party a contract with appropriate data protection clauses was not always in place.

! Some surgeries' websites contained only limited or very general fair processing information or details of cookie use. With the increasing use of website forms for patients to provide surgeries with information, and the use of websites as a mechanism to provide patients with information in advance of a visit, privacy statements need to be appropriately detailed and prominent.

! Surgeries were aware of standard NHS guidelines and timeframes for records retention and disposal, but there was a general lack of specific local procedures or protocols to review files and meet these standards.

! In some cases, in-house shredding of confidential waste was not effective with backlogs of files for disposal, and the volume of waste to be shredded was potentially more appropriate for a specialist third party contractor.

Case study - Secure destruction of personal data.

At one surgery where confidential waste was handled by a third party company, the contractor provided lockable consoles and arranged to shred waste on site. A certificate of destruction was provided to the surgery and retained by them as evidence of secure destruction.

The practice manager also observed the onsite shredding by the contractor, on an ad-hoc basis, to ensure it was completed in line with the contract.

! Several surgeries allowed unrestricted internet access by staff, including access to personal email/webmail accounts with the increased risk of data leakage, hacking and viruses. Where present local policies on acceptable internet and email were not always reflected in the software/tools that enforced them, which were usually applied by CCG-level IT providers.

! All surgeries visited used fax machines and some had fax policies and procedures in place, including the use of coversheets, pre-set numbers, telephone confirmations and 'safe harbours'. Staff awareness of these processes varied, as did awareness of secure alternatives to faxing such as the facility available to users of registered nhs.net email accounts allowing them to send faxes using their email client. Fax errors can produce serious breaches of the Act and result in sensitive medical details of patients being disclosed and possible civil monetary penalties being imposed by the ICO.

! Although USB sticks were not in common use, unsecured USB ports still created a risk of unauthorised removal of personal data using portable media or the introduction of malware and viruses to the network. Similarly in some cases local desktop C: drives could allow data to be saved on equipment and DVD/CD drives were enabled. The precise build and the mechanisms to lock down ports and drives was usually defined outside surgeries by ICT providers which included contractors and CCGs.

Case study – Endpoint control and USB.

At one surgery, the CCG had provided an approved encrypted and password controlled USB pen drive for use by surgery staff to securely move data. The process was overseen locally by the Practice Manager, who ensured the devices were kept secure and allocated appropriately.

Desktop PC units were locked down preventing the use of any other USB devices.

! Paper medical records were a challenge to manage at most locations due to the amount of space they take up. Records were usually held in

lockable filing cabinets or in separate lockable areas. However, the security and quality of these storage areas varied a great deal depending on the design of the surgery buildings and whether or not staff made appropriate use of the facilities available to them by locking rooms and cabinets.

Sources of information

The ICO has produced a range of guidance for organisations that GP surgeries can use to better manage and secure their personal information. Other guidance is available from the Health and Social Care Information Centre and NHS England.

A practical guide to IT security
www.ico.gov.uk/for_organisations/data_protection/~/media/documents/library/Data_Protection/Practical_application/it_security_practical_guide.ashx

A checklist of security measures to protect the personal data organisations hold
http://www.ico.org.uk/for_organisations/data_protection/security_measures

A quick guide to the ICO's code of practice for employers
www.ico.gov.uk/for_organisations/data_protection/topic_guides/~/media/documents/library/Data_Protection/Practical_application/quick_guide_to_the_employment_practices_code.ashx

A code of practice on the use of CCTV cameras
www.ico.gov.uk/for_organisations/data_protection/topic_guides/~/media/documents/library/Data_Protection/Detailed_specialist_guides/ICO_CCTVFINAL_2301.ashx

A checklist for handling requests from individuals to see copies of the information about them
www.ico.gov.uk/for_organisations/data_protection/~/media/documents/library/Data_Protection/Practical_application/checklist_for_handling_requests_for_personal_information.ashx

A code of practice on the collection of personal information and the notice that needs to be given to the individual
www.ico.gov.uk/for_organisations/data_protection/topic_guides/~/media/documents/library/Data_Protection/Detailed_specialist_guides/PRIVACY_NOTICES_COP_FINAL.ashx

NHS England advice on fair processing information and care.data
http://www.england.nhs.uk/wp-content/uploads/2013/11/cd-fair-pro-guid.pdf

NHS Safe Haven Briefing: Secure transfer of personal identifiable information by fax
https://www.igt.hscic.gov.uk/WhatsNewDocuments/Safe%20Haven%20Briefing_June2013.pdf

The IG Toolkit requirements as relevant to GPs
www.igt.hscic.gov.uk/RequirementsList.aspx?tk=416176775996226&lnv=2&cb=6d1de4de-db93-43d5-8d74-c204041a4026&sViewOrgType=4&sDesc=General Practice

The latest version of the IG Toolkit incorporates an IG incident reporting tool which helps align reporting arrangements and ensure automated notification to relevant regulators such as the ICO where appropriate
https://www.igt.hscic.gov.uk/WhatsNewDocuments/IG%20Toolkit%20V11%20Change%20Release%20Note%20(07%2006%2013)QC.pdf

A user guide to the reporting IG reporting tool
https://www.igt.hscic.gov.uk/resources/IG%20Incident%20Reporting%20Tool%20User%20Guide.pdf

Further assistance

The full range of guidance is available on the ICO website here:
www.ico.gov.uk/for_organisations/data_protection.aspx

The ICO also has a helpline with staff on hand to answer queries about data protection compliance on 0303 123 1113 or they can be contacted by email at casework@ico.org.uk.