Findings from ICO audits and reviews of community healthcare providers

June 2013 to December 2014

Information Commissioner's Office

Introduction

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 purpose of this report is to identify the issues that community healthcare providers are facing in relation to data protection compliance and provide good practice recommendations on how to overcome them.

This report includes an analysis of the serious data breaches reported by community healthcare providers. It also highlights five top tips for providers, based on the ICO good practice team's audit and information risk reviews in the sector.

The report should prove well-timed, coming during a time of great change in the provision of health services.

A majority of NHS care is already provided in people's homes and communities and more than 250,000 people are employed to deliver those services in England.

Community healthcare providers will be at the forefront of the move towards more integrated and coordinated health and social care services. This will bring innovative methods of delivering healthcare, but also bring with it new challenges around how patient information is handled when staff are out in the community.

Analysis of breaches

Since June 2013, all English health service organisations processing health and adult social care personal data are required to report serious data breaches using the Health and Social Care Information Centre (HSCIC) reporting tool.

Serious incidents (often referred to as SIRIs – Serious Incidents Requiring Investigation) are categorised into three levels, based on their severity. Details on how these incidents are defined are included in an appendix to this report.

The ICO is notified when incidents in the highest category (known as level 2 SIRIs) are reported. That means a number of information governance issues, such as the loss of one person's information on a home visit, may not be reported to the ICO through this system. Such incidents are not included in this analysis.

It's worth noting that these figures only refer to England. Health service bodies in Scotland, Wales and Northern Ireland are not currently required

to notify HSCIC of breaches through the reporting tool (though they should still submit a report to the ICO using our security breach notification form available on our website).

We analysed reports made by community healthcare providers between June 2013 and June 2014. We excluded mental health trusts, as these are not always solely community healthcare providers, and can face different information governance challenges.

The most striking – and reassuring - finding was that only 8 per cent (34) of all of the reports the ICO saw related to community health providers. We also found:

- 24 of these related to paper based information
- Only 5 of these related to deliberate or reckless disclosure or unauthorised access. Most related to information lost, disclosed or mislaid in error
- 10 related to digital information, of which 9 were categorised as disclosed in error
- In cases where electronic information was involved, more information was generally disclosed per breach reported.

Example
The number of people affected by a breach can vary dramatically. One reported community health incident involved over 100,000 items of data disclosed in error electronically, another over 3,000 items of patient information shared via unencrypted email.

Careless error or something more?

Our audits and information risk reviews highlight that community healthcare services breaches often relate to a low number of affected patients.

Digital information 'disclosed in error' commonly included cases such as sending emails to correct recipients but via unencrypted email addresses, or emailing via encrypted email but to the wrong recipient. However in one case, a clinician sent an unencrypted email containing patient information to an all staff email list.

Conversely, breaches relating to paper based information were notified for a variety of organisational reasons typically including loss or mislaying of paper patient files, failure to dispose of historic paper records and inability to locate live paper records within an organisation.

A significant number of reports relating to paper based information relate to simple physical loss of bags or briefcases containing patient notes by employees on public transport or mislaid in other public spaces, such as found in streets or shops or disused offices.

The remainder were notified for a variety of other reasons including basic employee procedural errors such as sending letters to the wrong address, wrong patient or faxing to the wrong number. Only one reported breach related to physical damage to paper records stores.

Top tips for community healthcare providers

The breach statistics above show the majority of incidents are as a result of either a lack of staff training or awareness, or from easily rectifiable technical or organisational issues. That trend continues in the findings of the ICO's good practice team visits.

The team's programme of audit and information risk reviews, from October 2013 to date, included four audits and three information risk reviews of community healthcare providers.

Through these visits - and broader discussions with community healthcare information governance professionals – it is clear there are particular challenges the sector faces. The primary issue is around providing services from multiple locations (some with a very large geographic coverage). This brings challenges relating to remote working and the security of manual and electronic data when staff work off-site.

We have drawn together the findings from our work, to highlight our top five common findings of areas for improvement. We've also included some good practice recommendations (marked with a ✓) intended to help providers who are processing personal data in similar circumstances.

1. Know what you hold and where

Our findings consistently showed that one of the key issues facing community healthcare providers is information mapping.

- ✓ By this we mean that organisations need to be aware of what personal data they actually hold, how that information 'flows' around the organisation, how long it should be held for, where it is and who in the organisation has responsibility for it.

  Without this mapping information, an organisation cannot know what records they hold and where they are located, and so cannot ensure that the records remain usable and secure for as long as they are required.

- ✓ Information mapping should include both electronic data (central and locally held databases, patient lists etc.) and also manual files, such as paper files or records held at outlying clinics.

- ✓ This is particularly important for multi-site providers, especially during cost reduction exercises, when outlying sites may be closed or amalgamated, and there is a risk of records being left behind or forgotten.

Example
When we visited outlying sites on one audit, we found 'abandoned' paper files. There had been no data mapping exercise, so no one knew which department they belonged to or who had responsibility for keeping or disposing of them.

- ✓ In this case our recommendation was to formalise and promote the use of a checklist in the organisation's Records Management Policy, which made sure premises being vacated or undergoing a change of use were checked to ensure personal data wasn't being left behind. This was accepted by the organisation.

- ✓ When information mapping at multi-site community healthcare trusts, we would recommend that all local sites should list information consistently and in an accessible format.

- ✓ This will enable the location of both electronic and paper based files to be recorded and tracked centrally and reduces the risk of files being mislaid, incomplete or inaccurate.

2. Ensure staff awareness of basic security

In our experience, staff awareness of basic security issues is key to reducing the number of serious data breaches.

- ✓ Ideally information security training should be provided for operational staff, including front line and records handling staff working within localities, at the start of their employment, to minimise the risk of errors, unauthorised disclosure or data loss.

- ✓ As a matter of good practice, this training should also be refreshed on a regular basis.

  Annual information governance training refresh is a requirement in England, as set out by the HSCIC, (and there is a welcome move towards this in both Wales and Northern Ireland). Organisations could look to adapt this training to include more bespoke information security

elements. There is currently a move to mandated regular information governance training, which we would welcome for community healthcare providers.

- ✓ We would recommend that information security training is provided at the earliest opportunity and in a consistent and auditable manner, to reduce the risk of staff making basic security errors.

- ✓ We've seen that local induction processes can vary widely from one locality to another, particularly if induction is carried out locally (and perhaps informally) by line managers rather than a central HR team.

Example
In one organisation, responsibility for induction fell to line managers as staff were so widely spread geographically. The induction included highlighting policies and procedures to new starters.

No one, including information governance staff, had an overview of what was provided at each local induction and there was no sampling of HR files to ensure that local inductions had been adequately completed and were on file.

- ✓ Our recommendation was that the information governance department should review the local induction process to ensure that information security and information governance were consistently and appropriately covered during induction, perhaps by adding a brief guide or checklist to the template.

The organisation agreed that its HR department would work with the information governance team on this recommendation.

- ✓ In addition to the checklist mentioned above, a brief reminder, one page sheet or handbook (e.g. for internal post always do x, for external post do y, for faxes refer to the Safe Haven policy etc) could be produced that could be referred to on an ongoing basis.

- ✓ In this example, this could then be used as an 'aide memoire' by both community based clinical staff and office staff taking paper records home or out of the office.

Fax and emails sent in error
Fax and email errors can produce serious breaches of the Data Protection Act and result in sensitive medical details of patients being disclosed - a number of the data breaches we analysed related to information being disclosed in this way.

Although this is not a problem unique to community health providers, the fragmented nature of working across multiple sites may mean that fax and email form a more central communication tool than in other organisations.

- ✓ You should ensure that, before using fax or email (for internal or external purposes), your staff consider whether it is a suitable means of communication, depending on the nature of the information and the harm that might result from unauthorised disclosure or access.

- ✓ Something as simple as double checking the email or fax address being used, or removing 'auto-suggest' for addresses from emails may have been enough to avoid some of the breaches we have reviewed.

- ✓ It is also key that monitoring and spot checking of staff regularly takes place to ensure that procedures are being consistently followed across sites. This will identify any hotspots of concern, where further training may need to be given, and help build a culture of following information security procedures as business as usual.

Example
During the ward visits on one audit, we established that although the organisation had detailed 'Safe Haven' faxing and postal policies and guidelines, ward and clinic staff actually had little awareness of these.

Our auditors saw no signage near the fax machines reminding staff of Safe Haven rules. There were also no consistent rules being applied for sending personal information by post between localities (for example whether personal data should be double enveloped or sent by hand or recorded mail).

- ✓ We recommended that the organisation ensure that notices highlighting relevant processes for securely sending personal data by fax are displayed by all fax machines.

The organisation accepted this, noting that its internal SharePoint system was being reviewed and amended, meaning that information in relation to using faxes would now be easily accessible.

3. Training

We consistently found that take up of data protection / information security training in the community healthcare sector is lower than in other providers, particularly in areas of the UK where achieving 95% training rates is not mandatory for an organisation. In such latter cases we have

found that there is inevitably less dedicated focus on training as finite resources are focussed upon other issues.

- ✓ Low training uptake generally may be due to the large geographic spread together with the off-site nature of work of a large number of community healthcare roles.

- ✓ If staff are widely spread out, perhaps consider the use of regular podcasts or webinars or the use of mobile technology to enable staff to access training / awareness materials.

- ✓ These remote methods of communication could also raise the profile of data issues on sites that are not regularly visited by the information governance team.

- ✓ We have also seen good practice such as the use of training workbooks for manual completion by staff who cannot easily access online training.

Turning to more specialised training, we also found in a number of cases there was no central records management function or specially trained staff, nor was there was specialised training for the staff who undertook the records management function in the localities.

Example
In one audit, we found that management and archiving of all patient records for one site was being done by one temporary staff member who had developed her own forms and processes but had had no records management training.

In addition to the risk that records may not have been managed properly due to lack of training, if she had left, the organisation would have faced a serious business continuity problem.

- ✓ Our recommendation was to establish consistent written procedures for each site within the organisation to standardise local practice as far as possible, and this was accepted by the organisation.

- ✓ To ensure good practice, we'd normally recommend implementing training pitched at an appropriate level (and if necessary differentiated by role) for both permanent and temporary staff with records management, archiving, disposal, or administrative responsibilities.

- ✓ For community healthcare providers, this should ideally also include basic awareness training for other 'front line' staff at local sites such as receptionists, administrative clerks and facilities staff.

- ✓ Front line staff are key when there is no dedicated records management / facilities staff at smaller sites, as they will likely be dealing with faxes, security, archiving and disposal of information and any requests for personal data that may be received.

4. Develop guidelines for taking patient or service user information off site

A number of data breaches reviewed related to information being lost or mislaid by staff who were off site, for example on their way to and from visiting patients or service users.

This included both manual data (e.g. patient records) and information held electronically (such as on a laptop or memory stick). It is clearly an area of information risk, especially as the nature of community healthcare involves a significant amount of off-site working.

- ✓ We'd recommend that in addition to implementing data protection / information security training, you should consider developing specific recommendations to ensure the security of data and equipment when staff work off-site, including guidelines for the handling of health records off-site.

- ✓ Staff should be reminded of their responsibilities to keep records safe and secure at all times.

- ✓ They should also be reminded of the possible risks of leaving medical records unattended and the consequences should their negligence result in a security breach.

- ✓ Staff should be made aware of these recommendations:

    - Consider if information really needs to be taken out of the office, or if less information could suffice

    - Consider if the information could be carried in an electronic form on an authorised and appropriately encrypted device.

    - Seek permission from line managers to remove hard copy information from premises.

    - Log the individual documents being taken from your premises and log them back in on return.

    - Carry the information in a non-transparent folder or secure locked bag.

- Keep other patients' information securely locked in the boot of the car when visiting individual patients.

- Always return information to the office for secure disposal.

✓ We would also recommend that if your organisation is spread across multiple sites that you consider alternative methods of raising awareness of information security amongst your staff. Good practice we have seen includes the use of cascade briefs by team managers, posters in receptions, quick guides attached to payslips and laminated notices near faxes.

✓ Once this is in place, it is important to ensure that there is monitoring of compliance with your organisation's information security procedures by line management to help identify any areas of risk.

✓ This is particularly key for management of information risks in outlying areas where working practices may not be easily monitored by the information governance team on a regular basis.

✓ You should also consider implementing a mechanism for escalating concerns up the management chain or to the information governance department - such as recording and review of monitoring outcomes.

Example
On one audit, both community based clinical staff and HR confirmed they took paper records home or out of the office.

Interviewees demonstrated awareness of basic security principles such as not leaving files in cars, or if this could not be avoided then locking them in the boot. However, it was reported that when visiting patients, files could be left on the front seats of cars for ease of access (especially when visiting multiple patients), and were kept in unlocked cloth bags.

✓ Our recommendation was to put processes in place to ensure that there was understanding of, and compliance with, home working policies by staff.

The organisation partially accepted this, noting that they had an initial authorisation and checking process for use of laptops and devices which had to be carried out prior to any member of staff having home access.

✓ We explained that this alone would not necessarily mean staff understood their responsibilities on an ongoing basis, so the organisation agreed to develop a staff information leaflet.

- ✓ They also agreed to look to have more frequent security checks on laptops and devices.

5. Ensure central oversight of the records management process

- ✓ A further key finding that is consistently seen on audits and information risk reviews of community healthcare providers is a lack of central awareness or oversight, eg by senior management or information governance, of the end-to-end responsibility for records management.

  An absence of appropriate oversight could lead to a risk of a fragmented and inconsistent approach to the records management process, with no one having overall control or responsibility.

  This is in contrast to Acute Trusts, which usually have a large central records library and a dedicated records management team with appropriate qualifications.

- ✓ It is particularly important to have central oversight when services are being delivered from multiple sites, perhaps spread over a wide geographic area.

  In these cases, if there is no defined process then our experience is that various differing records management and archiving processes tend to be developed locally on each site.

  This can lead to confusion over what is the right approach (for example, how to dispose of confidential information, how to secure store files or methods of archiving).

  This in turn makes it harder for mislaid files to be located, or for the central information governance team to establish what has happened in the case of an information breach.

- ✓ Central oversight could be achieved by having a review of records management as a standing agenda item at information governance meetings, having key performance indicators relating to records management (such as archiving backlogs, loss of files etc) regularly reported to senior management, regular feedback from local area managers and so on.

Example
A community healthcare provider had multiple methods of disposing of confidential information across sites including shredding bins, shredding

bags, personal non cross cut shredders, external shredding companies, and via office landlords.

No one knew what the right method of disposal was. When staff moved sites, there was a risk they used their own way of disposing, which may not have been appropriate - in one case, local process was to leave bags of confidential waste out in an unlocked bicycle shed awaiting disposal.

- ✓ We recommended that the organisation should rationalise confidential paper waste destruction methods, and introduce a single cross-organisation mechanism and policy.

- ✓ We also asked the organisation to consider one central role or function be mandated to hold central copies of all destruction certificates in order to provide an audit trail and to update their information asset register. The organisation accepted both these recommendations.

- ✓ We recommend that staff across sites are aware of procedures, and that there is some method of checking or dip sampling to ensure they are being implemented.

Sources of information

The ICO has produced a range of general guidance for organisations that community health providers can use to better manage and secure their personal information. You can find this guidance on our website, ico.org.uk, with particular health guidance at ico.org.uk/health

Further assistance

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.

Appendix

Since June 2013, all English health service organisations processing health and adult social care personal data are required to report serious data breaches using the Health and Social Care Information Centre (HSCIC) reporting tool.

This is done through the Information Governance Toolkit platform. Serious incidents (often referred to as SIRIs – Serious Incidents Requiring Investigation) are categorised into three levels, based on their severity. Level 0 or 1 SIRIs are managed in accordance with an organisation's local procedures and are not reportable, while the ICO receives notification emails regarding incidents marked as level 2 severity.

There is no one simple definition of a serious incident. The HSCIC provides guidance to organisations in their Checklist Guidance for Reporting, Managing and Investigating Information Governance Serious Incidents Requiring Investigation, which is available on their website.

The HSCIC guidance also contains definitions and examples of breach types; users have to select the most appropriate category when reporting a SIRI.

Some breaches may of course fall within more than one category. The HSCIC advise that for reporting in these cases, one description which best fits the key characteristic of the SIRI should be selected.

Breach categories – HSCIC guidance:

A	Corruption or inability to recover electronic data
B	Disclosed in Error
C	Lost in Transit
D	Lost or stolen hardware
E	Lost or stolen paperwork
F	Non-secure Disposal – hardware
G	Non-secure Disposal – paperwork
H	Uploaded to website in error
I	Technical security failing (including hacking)