Findings from ICO advisory visits to residential care homes for adults and children

September 2015

Contents

Executive summary

The Information Commissioner's Office (ICO) is the regulator responsible for ensuring that organisations comply with the Data Protection Act 1998 (DPA) and for promoting good practice in information handling. The Act consists of eight principles with which all organisations processing personal data must comply.

During 2014, the ICO (Good Practice department) undertook 10 voluntary data protection advisory visits with residential care homes. The scope of these visits focussed on the technical and organisational measures in place to address the following key issues:

- Security of personal data
- Records management
- Data sharing

The objective was to understand how these organisations are processing personal data. This report is aimed at all residential care homes and other organisations that provide similar services and includes guidance and advice to help them improve their data protection practices.

This report explains the areas where residential care homes appear to be performing well, as well as highlighting the common problems and areas for improvement that other organisations can learn from. The report also includes further guidance and advice to help organisations improve their data protection practices.

Summary of findings:

- There was little if any formal training for data protection and associated issues such as security of personal data and records management.
- The use of shared generic accounts to gain access to IT systems was widespread.
- Where system access was password protected these were seldom complex. Passwords were also not changed regularly.
- Encryption of personal data held on portable devices was often not implemented.
- There was little in the way of formal policies and procedures in place for data protection and even less for data sharing specifically.
- End point security that restricts the use of portable media to transfer data was rarely applied to computers.
- Retention schedules were seldom in place and often only applied to manual records.
- Adequate information for individuals about how the organisations were going to process their personal data was not always supplied. There

were instances of where processing information was written, but was not communicated to residents as well as it could have been.
- Physical building security is generally good with access and movement within premises being managed through controls, such as manned receptions, visitor procedures and appropriate siting or obscured views of hardware processing personal data.

Main recommendations, themes and observations

Through working with residential care homes we were able to gather information about the challenges and areas of good practice that were in place. Below are the key findings from our visits. These are provided in order of the frequency we encountered them:

1. Training

Training is a key tool for any organisation in ensuring that staff are aware of their responsibilities for data protection. There was little formal data protection training in the residential care homes we visited. Where training did take place it tended to focus on care standards for the use of information rather than data protection requirements.

Key elements of good practice for data protection training include:

- mandatory induction training that ideally takes place before allowing staff to access personal data;
- mandatory annual refresher training;
- annual reviews of data protection training content to ensure that it is up to date and remains relevant to the residential care home needs;
- specialised training for key roles, for example those dealing with requests for personal data, information security, or records management;
- training logs that record completed data protection training; and
- procedures to ensure that incomplete training is monitored and addressed.

Did you know?

We've produced training videos to help organisations deliver training to their staff.

http://ico.org.uk/for_organisations/training

We also have a selection of material than can be printed and used to improve awareness of data protection issues for staff.

https://ico.org.uk/for-organisations/training-materials/toolkits/

The National Archives has produced a free e-learning training resource for small to medium enterprises called 'Responsible for Information' which contains practical considerations for staff handling personal and other information:

http://nationalarchives.gov.uk/sme/index.htm

2. Retention schedules

Under data protection legislation, organisations should not hold personal data for longer than necessary.

Some of the residential care homes we visited had a retention schedule in place but only applied it to their manual records, which results in the risk of electronic client records being retained for longer than necessary.

Retention schedules and associated policy should:

- apply to both electronic and manual records;
- justify the retention of records based on the type and any business or legislative need;
- set out how any exceptions to retention schedules are applied and reviewed;
- specify who is responsible for destroying records;
- list appropriate disposal methods and security requirements;
- set out the requirements for recording records as destroyed; and
- require periodic review to ensure the retention schedule is correctly applied.

Case study – retention

One of the residential care homes that we visited had a complete set of retention schedules in place for all the categories of information that they processed. While little of the personal information had reached the end of the retention date they were already appropriately prepared for identifying and disposing of information that was no longer required.

Did you know?

Applying retention schedules to personal data is a legal requirement under the Fifth Principle of the Data Protection Act 1998.

http://ico.org.uk/for_organisations/data_protection/the_guide/information_standards/principle_5

3. Fair processing information

Organisations are legally required to advise individuals as to how their personal data will be used and who it will be shared with. It is also good practice to tell people how they can access their personal data.

Most of the residential care homes we visited did not inform individuals about how their information would be used and who it could be shared with. Some of our visits raised concerns about the effective communication of fair processing information to individuals.

Did you know?

Further information about privacy notices required to provide fair processing information to individuals is available on our website:

http://ico.org.uk/for_organisations/data_protection/topic_guides/privacy_notices

4. Encrypted email

While electronic information is in transit encryption reduces the risk of successful interceptions to the personal data. Encrypted information also reduces the risk of personal data being accessed inappropriately if sent to the wrong email address.

Few of the residential care homes that we visited had encrypted email solutions in place, despite the sharing of sometimes sensitive personal data. Where they were in place they were often at local authorities insistence to allow personal information to be shared. Also there were inconsistencies in implementation, with some care homes using encrypted email when dealing with a local authority but not when dealing with other care homes.

5. System security

Restricting records access to only those that require the information helps protect individual privacy. The use of complex, periodically changed passwords allows organisations to reduce the risk of unauthorised access

to personal data. Ensuring that these protections are active and updated regularly is an essential guard against cyber attacks.

However, many of the residential care homes that we visited had limited IT resources often held in a single office.

Many used generic shared logons for staff to access the system. By using individual logons for staff, care homes can not only restrict what information is available to staff, but also implement audit trails to track staff access to and editing of information.

Passwords that were in place were seldom complex (over eight characters, a mix of upper and lower case, and containing numbers and unusual characters) and were also not changed regularly.

The support for IT solutions varied across the homes that we visited. However, even residential care homes with the most basic of IT solutions reported that they had up to date anti-virus/ malware in place as well as firewalls. PCs are often sold with these elements as standard, and there are resources on the internet which can be used to obtain free versions of these measures.

Did you know?

We've produced a practical guide to IT security which is idea for small business:

https://ico.org.uk/media/for-organisations/documents/1575/it_security_practical_guide.pdf

6. Incident reporting

Residential care homes regulated by Ofsted are required to have an internal incident reporting procedure. Formal internal incident reporting allows organisations to monitor incidents, assess their frequency, identify potential weaknesses in processes and decide on what remedial action is required.

However, from our discussions it appeared that these procedures were around reporting care incidents internally and that information incidents such as the loss of personal data would not be included. In smaller residential care homes where the frequency of incidents should be very low, it is important that the focus is on ensuring that staff will recognise

and report possible information incidents, for example loss or inappropriate disclosure, and any near misses, to prevent recurrence.

Did you know?

More information is available about how to handle a security breach:

https://ico.org.uk/for-organisations/guide-to-data-protection/principle-7-security/#breach

We've also produced guidance on data security breach management and notification of data security breaches to the Information Commissioner's Office:

https://ico.org.uk/media/for-organisations/documents/1562/guidance_on_data_security_breach_management.pdf

https://ico.org.uk/media/for-organisations/documents/1536/breach_reporting.pdf

7. Encryption of portable devices and media

Portable devices that store personal data (for example laptops, USB sticks and DVD/CD media) pose a high risk to data security and should use encryption to protect the information.

Very few of the residential care homes we visited implemented encryption methods to protect personal data held on such devices. Between 2010 and 2014 the ICO issued nine civil monetary penalties totalling £1,100,000 in cases where personal data held on portable devices was not encrypted.

Did you know?

For more information about our approach to the use of encryption to enhance the security of personal data:

https://ico.org.uk//for-organisations/encryption/

8. Data sharing

Residential care homes are required to receive and share personal data from or with other organisations. This can include inter-agency meetings where multi approach care plans are discussed and put in place for residents.

The majority of care homes we visited did not have formal policies and procedures in place to support that sharing.

By implementing formal data sharing arrangements residential care homes can:

- stipulate when information can be shared;
- specify what security measures need to be in place;
- specify who is allowed to authorise data sharing;
- require records of sharing to be maintained; and
- ensure requirements for dealing with subject access requests or, where applicable, freedom of information requests are specified.

Establishing formal agreements with organisations sharing data allows residential care homes to mandate how the information will be processed over its lifecycle, including how it is disposed of. Reviewing these agreements regularly ensures they continue to meet the organisation's requirements.

Case study – formal agreements

One of the residential care homes visited had a four page information sharing agreement, which was being circulated around the key partners, such as the youth offending team, police and local authority, for sign off.

Case study – telephone requests for data sharing

Staff in one care home demonstrated a good knowledge of sharing client personal information over the telephone. When telephone requests for information were received staff would establish the identity of the caller, ensure they had a legitimate purpose to request the information and subsequently log the request along with any decisions about sharing.

Case study – minimising information

The majority of staff that we spoke to said that they would only share the minimum personal information required. By ensuring the personal information shared is not in excess of requirements, they reduced the likelihood of an incident such as excessive disclosure of personal information and further protected the privacy of their clients.

Did you know?

We've produced a statutory data sharing code of practice:

http://ico.org.uk/for_organisations/data_protection/topic_guides/data_sharing

9. Data protection policies

The use of formal policies and procedures is essential for any organisation to ensure compliance with data protection requirements.

Most residential care homes did not have formal policies and procedures in place for data protection or related subjects such as information security and records management.

Policies and procedures that are tailored and proportional to an organisation's compliance needs inform staff of how personal data should be processed. Topics might include:

- fax usage;
- email usage;
- manual document disposal;
- physical security;
- homeworking;
- retention;
- system access;
- dealing with disclosures over the telephone;
- archiving;
- data back up and retrieval;
- incident reporting; and
- training.

10. End point controls

Portable media solutions allow large amounts of personal data to be removed instantaneously, as well as allowing the transfer of malware onto an organisation's systems. Most of the residential care homes that we visited did not have measures in place to restrict access to USB ports and DVD/CD drives. This poses a significant risk to the security of personal data.

By locking down the use of USB ports and DVD/CD drives, residential care homes can mitigate the risk of loss of personal data and the transfer of malware onto systems.

Where access is allowed it is good practice to:

- identify the specific business need to copy information to USB sticks or DVD/CDs;
- restrict the access to roles where it is required;
- restrict use to specific approved devices;
- ensure staff access is appropriately approved and recorded;
- record and review logs of any information transfers to USB devices or onto DVD/CDs; and
- regularly review staff access to ensure it is still required or has been removed.

In many cases it would be preferable for the operating system to prevent use of these facilities altogether.

11. Fax machines

The enforcement action the ICO has taken indicates that fax machines are still a significant risk to organisations. Sending information by post or fax to the wrong recipient was the third most common type of incident in quarter four 2014/2015.

Although the use of fax machines by the residential care homes we visited was low, their ongoing use means that they need to consider the risk of wrongly disclosing information.

Implementing a fax usage policy can reduce the associated risks. Where faxes are used it is good practice to:

- require a pin or swipe card for access to prevent unauthorised use of the fax machine;
- have pre-programmed numbers to key external contacts to prevent misdialling;
- limit the number of machines;
- restrict the information (for example, limit the amount of personal data) allowed to be sent;
- require the recipient to confirm they have received a test page before sending personal information; and
- require the recipient to confirm they have received the information so that any losses can be identified and investigated quickly.

Removing fax machines and preventing their use in favour of secure electronic transfer solutions is better practice.

12. Physical security

Ensuring that access to premises and offices storing and processing personal data is secure reduces the risk of unauthorised access to that data.

The majority of residential care homes that we visited displayed good levels of physical security.

Good examples included:

- secure premises where access to visitors was restricted and visitors had to be signed in and escorted;
- offices where personal data was stored were staffed, or locked when unattended;
- locked filing cabinets with access restricted to staff on duty; and
- preventing unauthorised access to offices by residents.

13. CCTV surveillance

Although the use of CCTV surveillance by care homes, residents or families was not examined during the advisory visits, this is an issue which was recently addressed in a CQC report. The ICO were involved in discussions with the CQC regarding the use of surveillance in relation to the report.

Where CCTV is used to deliver surveillance the ICO believes that its use should be a proportionate response to a pressing need.

Did you know?

The CQC's report into the use of surveillance:

http://www.cqc.org.uk/content/using-surveillance-information-service-providers

The ICO has published a CCTV code of practice:

https://ico.org.uk/for-organisations/guide-to-data-protection/cctv/

Further action

While this document highlights the key issues that residential care homes should consider, it is not an exhaustive list. Residential care homes must

be aware of the risks and requirements involved in processing personal data and ensure they implement adequate measures to deal with these.

More information

The ICO has produced a range of guidance that residential care home organisations can use to better manage and secure their personal information:

- Data protection guidance

Other useful guidance

- A practical guide to IT security
- Employment code of practice – quick guide
- Checklist for handling requests for personal information

Find out more about our advisory visits and read summaries of advisory visits we've carried out.

Advice and assistance

The ICO also has a helpline with staff on hand to answer queries about data protection compliance on **0303 123 1113**.

Appendix A

Background

The ICO is the regulator responsible for ensuring that organisations comply with the DPA and also has a remit for promoting good practice in information handling. The Act consists of eight principles with which all organisations processing personal data must comply.

In 2014 the ICO undertook 10 advisory visits to a selection of adults and children's residential care homes to get a better understanding of the processing of personal data they undertake and the circumstances in which they operate. Advisory visits are a one day informal visit to look at how an organisation handles personal information. ICO staff provide practical advice and guidance on site and a short report after the visit. The visits focused on information security, records management, and data sharing.

Each of the residential care homes visited were eager to work with the ICO to improve their compliance with the DPA. They had already considered their requirements and had put some measures in place.

Where residential care homes do not implement adequate measures to comply with the DPA they could face enforcement action by the ICO. For serious breaches this may result in a civil monetary penalty of up to £500,000.

Approach

We approached 80 residential care homes to offer them advisory visits. Of these 10 accepted our offer and subsequent visits were scheduled from July to December 2014.

Typical processing of personal data

Both adult and children's residential care homes process information about their residents in paper and electronic form. This can include initial referrals, background information, care plans or sometimes sensitive medical information such as medication requirements. While our work focussed on care homes that provide adult or children's residential social care services, we believe that many of the issues highlighted in this report are equally relevant to residential homes providing other services.

Appendix B

Children's residential care homes

The Care Standards Act 2000 (CSA) defines a residential children's home as an establishment that provides care and accommodation wholly or mainly for children. Children are defined by the CSA as anyone under the age of 18. Homes can provide either long or short term residential care. They can also provide specialist care for children with:

- disabilities;
- emotional or behavioural difficulties;
- mental health conditions; and
- drug or alcohol conditions.

Ofsted regulate and inspect children's residential care homes. They are subject to inspections without notice. As part of the review Ofsted will inspect records to use as evidence of the quality of care that is provided. There are also requirements under Ofsted guidance to ensure that personal data is accessible and available where appropriate for the child.

Where a children's home includes the provision of healthcare it is subject to the Health and Social Care Act 2008 (HSCA). If the home provides services that must be performed by a qualified healthcare professional it is required to be registered by the Care Quality Commission (CQC).

There are specialist child residential care homes (for example, care for children who have been victims of abuse) that process highly sensitive personal data that can be detrimental to individual's wellbeing if not processed carefully.

The children's residential care homes that we visited were independent, providing outsourced services for children and young people up to 18 years old in local authority care. They provide support and prepare young people to move to their onward placement, return to their family home, or make the successful transition to independent living.

Adult care homes

There are two types of adult care homes, residential and nursing. Residential care homes can vary in size from very small homes with a few beds to large scale facilities. They offer care and support throughout the day and night. Staff are on hand to help residents with washing, dressing, at meal times, and using the toilet.

Nursing care homes also provide 24 hour medical care from a qualified nurse. They can also provide for specialist requirements for example, dementia care. They therefore need to process large amounts of sensitive personal information about their residents.

Adult care homes have to be registered with the CQC. CQC inspect residential care homes for adults which provide social care. These visits may include accessing personal records to ensure that care has been properly documented.

Other residential homes

Residential homes that do not provide social care services (for example, a home for ex-young offenders) are not governed by Ofsted or the CQC. We visited a small number of these homes. However, as with all residential care homes they have to process personal data in line with data protection requirements.