Housing LIN
Connecting people, ideas and resources

Viewpoint 84

Extra Care and the changing face of Data Protection Compliance - More requirements, or just different ones?

This viewpoint for the Housing LIN sets out the challenges and potential areas of weakness facing extra care settings with meeting the current Data Protection Act and the increased compliance set down in the General Data Protection Regulation.

Written by **Lesley Cooley** of Audit and Risk Professionals for the Housing Learning and Improvement Network

January 2017

Which Data Protection Regulation are we working to?

The Data Protection Act 1998 (DPA) is the current legislation that the UK uses to legislate Data Protection compliance. The Information Commissioner's Office (ICO) is the regulatory body which oversees compliance, holds the register of Data Controllers and provides advice to individuals and companies on good practice. The General Data Protection Regulation (GDPR) is the new European wide regulation and comes into force in May 2018. The Secretary of State, Karen Bradley MP, has confirmed that as Britain will be part of the EU when the GDPR comes into force in 2018 we will therefore need to meet the requirements of the new regulation. There are a number of major changes that the GDPR brings into place, some of which are allowing individuals greater control over their information and a requirement for organisations to take steps to protect that information better, be more transparent about the use of that information and more accountable for their compliance with the regulation, as well as increased financial penalties for non-compliance.

Extra care services and their unique challenges

Extra care services usually involve a number of agencies in an individual's care, this requires the sharing of information across a varied group of staff and organisations. This can be a challenge from a number of perspectives, from collecting the information, sharing it and securing it prior to destruction. One of the key things to ensure, from a data protection aspect, is therefore ensuring that there are relevant permissions in place to share and protect the service user's information. Much of the information that is shared within an extra care setting is considered "sensitive personal data"; that is, information that relates to an individual's physical or mental health or wellbeing. As this information is so sensitive there is a requirement for additional safeguards to be put into place to protect this information from becoming known to those who should not have access to it.

Contracts should be in place between the various stakeholders to set down the responsibilities of each party. One of elements of the contract should relate to how to share information and maintain the confidentiality of it. The clauses in these contracts are usually quite weak and vague. Under the GDPR, contracts are required to clearly show responsibilities of the stakeholders, there is not the option of negating responsibility for the information you have access to. This is a change from the standard DP clause which basically says that the stakeholders will meet the requirements of the Data Protection Act; this clause when used also doesn't protect either party.

Contract clauses should protect the organisation, the individual's information and set out the basis for sharing and disseminating information. Contracts should include a clause whereby the parties to it have to notify within a set period the other parties if there is a data breach within their organisation. The breach indicates to the other parties in the contract potential weaknesses in the data protection framework and can alert you to issues which may not yet have caused a breach within the contracted services but highlight areas for concern. There also need to be clear guidelines as to who the information belongs to and the conditions for sharing, retaining and destruction.

What does Data Protection mean to the people doing the job?

We live in an environment where people openly share information through a variety of forums such as Facebook, Pinterest, Instagram, Twitter etc, yet when we share information with an organisation we expect them to take great care of it and not to share it unnecessarily.

Data protection will mean different things to different people depending on their personal experiences, any training they have received and the type of information that they are dealing with. The challenge most organisations have is raising awareness about the best way to secure information. Most of the breaches investigated by the ICO are as a result of human error, in that an individual has accidentally released information to someone who should not have received it. Another common type of breach is the deliberate theft or release of the information, usually by a member of staff. Morrison's and Lex Autolease have both been victims of this type of information breach. A disgruntled Morrison's employee released online personal information including salary information, dates of birth and national insurance numbers. The employee from Lex Autolease gathered information about customers who had been in accidents and sold it to a third party as personal injury claim leads.

Records come in two forms, paper or electronic. There are benefits to both types of record. Electronic records are easily portable, can be password protected (or, even better, encrypted) and easily distributed (both a benefit and a risk). In addition, whatever electronic device is used is also attractive to thieves, not because of the information held on it but because of the hardware. Paper records cannot easily be changed, are portable and easily disposed of by shredding. Additionally, it is rare for paper records to be stolen, although they have been left on buses, in filing cabinets sold at auction or buildings which have been sold (the organisations ended up with financial penalties as a result!).

Collecting, storing and sharing information brings a whole set of issues around the security of that information. As you have collected the information you have the responsibility of ensuring its security. How do you do that?

When information is collected on a portable device such as a tablet, phone or camera, you need to think how this information will be secured should the device be lost or stolen. Depending on whether the device is the property of the organisation or belongs to a member of staff can denote the options that are available to you. For example, remote swipe (the ability to remove all the documents, settings and information from a device via a remote connection) can be used for organisational equipment or with the permission of the device's owner but it is not always effective and needs to be undertaken as soon as the device has been reported as missing. Encrypting the device is the safest way to ensure that the information held on it is secure in the event that the hardware falls into the wrong hands. Password protection is insufficient to safeguard the information held on the device.

Email is a common method of sharing information and there is a common misunderstanding about the security of email. People often think that sending an email keeps information secure, especially if it is between people in the same organisation. This stems from a belief that emails between employees in the same organisation don't go outside the organisation, but this is only correct if the organisation has a specific email server in-house. More often than not that email is going out to "the cloud" and then coming back in. Email is like a postcard, it can be intercepted and read by anyone who wants to read it, unless it is encrypted. So before someone sends something by email, they should be considering whether they would be happy to share that information.

Many corporate mail packages have the ability to encrypt emails or there are some packages available that will encrypt emails you want to send. If you are sending emails with sensitive personal information, you should be looking to encrypt that information. Some Local Authorities and Health Authorities use encryption software so replying to an encrypted email usually encrypts the reply.

Additionally, there have been a number of breaches where information has been sent to the wrong recipient. This is very easily done when a mail service "suggests" potential recipients for

the email, especially if you have more than one person with a similar name held in the contact list. For example, the prison service in Wales emailed the details of over a 1000 prisoners to someone inadvertently. The process for checking outgoing emails was so poor that they didn't send the email once but on three separate occasions to three separate individuals. The ICO fined the Prison Service £140,000 for not having robust checking procedures in place.

Each member of staff should have their own login to the electronic systems used within the organisation and the password should be changed on a regular basis. We have visited organisations where the password is posted on a sticky note by the machine so anyone can log in and access information, hardly providing assurance of data security! There have also been occasions where departments have used a "communal" login to gain access into systems.

The challenge in the extra care environment can be that records are moved from one location to another. I remember going to see a social worker about a possible fraud in an extra care setting some time ago and she gave me a lift to the station in her car afterwards. The back seat of the car was full of paper files relating to individuals for whom the social worker was acting. These files contained name, address, financial, health and social details about the individual, so not the most secure environment for records to be transported. A care home in Northern Ireland has recently been fined £15,000 for the theft of a laptop from the Manager's home. The laptop contained the details of 75 people (29 residents and 46 staff) but had not been encrypted so the theft meant that the person stealing the laptop had easy access to that information.

Organisations are moving towards an electronic means of recording the work they are doing with stakeholders, and how this is managed can be key to ensuring the security of the information. Many organisations now only provide access to the client records that the employee is visiting and this access is on a one record at a time basis, so that only one record is at risk at any one time. This is quite sophisticated but possible with the software available to organisations.

Policies, Procedures and Training

There are three elements which demonstrate a commitment to the Data Protection Act and are key to protecting the organisation in the event of a data breach as they are the elements that the ICO will review first. These are policies, procedures and training.

The organisation should have robust policies in place regarding data protection including confidentiality, data sharing and subject access requests. These policies should be communicated to staff on a regular basis and documented. The policies should also be reviewed on a regular basis and notated with the last review date so you can ensure that they are kept up to date.

Once robust policies are in place, the procedures to support them should be clear. Many organisations have come to the attention of the ICO because the processes to protect information were weak or not followed. Examples where organisations have come to the attention of the ICO due to a data breach include faxing information to the wrong destination, emailing information but forgetting to BCC the recipients, using personal devices without setting out how to store the information collected and giving information over the phone to someone who wasn't entitled to receive it.

Finally, there should be a training programme in place. It doesn't have to be a big formal training process, it can be as simple as discussing it regularly at staff meetings, just make sure that it is minuted as the ICO may ask for evidence that awareness training has taken place. If you are running a formal training programme, it should happen on a regular basis, preferably annually.

Rights of the individual

The rights of individuals are paramount under the Data Protection Act and they must be told what information about them is being collected and how it will be used (in the terminology of the act “processed”). Even if you need the information to be able to provide a service you should inform the person providing it how the information will be stored, how long for and who it will be shared with.

The GDPR further increases individuals’ rights to control their information. In practice this will mean that organisations need to safeguard information better, be more transparent about the use of that information and more accountable for their compliance with the regulation.

All individuals receiving Extra Care services can find out, under the DPA, what personal information a care provider holds about them by making a subject access request (SAR) to the care provider. That includes information made available to agencies working for them. Failure to provide all the information or withholding some of the information may result in a penalty being imposed by the ICO.

Mental Capacity Act and Data Protection

The requirements of the Data Protection Act give an individual rights around their information and how it is shared. Should the individual lack the capacity to understand how their information will be used, the permission of a representative (usually someone holding a power of attorney, or a parent in the case of a child) can be sought.

Where a representative seeks access to the personal records of the individual lacking capacity, when the request is made, the organisation will need to ensure that the person has legal capacity to act on their behalf and that the information they are requesting is in the best interests of the individual.

Right to be forgotten

The General Data Protection Regulation brings in more rights for the individual to ask for their information to be erased. This means that on meeting certain conditions, for example, if the individual removes their permission for you to have the information or the information is no longer required, it should be deleted. The deletion should take place without “undue delay” and be complete. This means that if you have shared that information with other organisations you have to take steps to notify them that the information should be deleted. It might be worth considering how you are going to do this at the point you start to share that information and formalise it within the contract.

Destruction of records

The DPA does not stipulate a minimum or maximum length of time personal information should be kept. However, The Care Quality Commission’s (CQC) recommendation is that information should be held for a period of seven years for adults from date of last entry, and eighty years for children from date of last entry. You can tailor your retention period to the type of records that you hold, but you should document what your retention periods are so that there is a clear guideline for the organisation.

The method of destruction for records should be compatible with the type of record. Paper records should be securely shredded. If you are paying a company to shred any records and they are taking them off site, they should supply you with a certificate to show that the records are securely destroyed. Electronic records should be fully erased from all computers, servers and back ups.

What happens when it goes wrong?

Let's hope you don't have a major data breach but you should have a plan for when things do go wrong. Firstly most data breaches are as a result of human error, which is people not following the processes and procedures which are designed to ensure that information is held securely. This can include emailing or posting the information to the wrong person, losing it or having it stolen.

Create a plan which can be put into action as soon as you identify the data loss. A plan should include basic details around:

- What information has been lost?
- Can we get it back?
- How did the loss occur and how do we stop it happening again?
- How do we notify the people whose information has been lost?
- Do you need to tell the Information Commissioners Office (based on severity)?
- Will you need a PR company to handle media enquiries?

Conclusion

Extra care services have many challenges around collecting, storing and sharing information from various sources, including service users, partnership organisations and contractors. Data Protection compliance can feel like an additional burden which makes record keeping a challenge. Substantially, the Data Protection Act is about having in place good practices and policies. To be able to effectively manage your data protection compliance you need to understand what information you are collecting and from what source, the sensitivity of that information, the areas where the information would be vulnerable to loss or theft and mitigate these through having good guidance and raising awareness through training.

About the author

Lesley Cooley of Audit and Risk Professionals is a qualified Data Protection Officer and has worked in the housing sector for over 15 years. Lesley provides advice to a range of housing providers including those with extra care services and may be contacted by emailing: ask@audit-and-risk.co.uk

Note

The views expressed in this paper are those of the author and not necessarily those of the Housing Learning and Improvement Network.

About the Housing LIN

The Housing LIN is a sophisticated network bringing together over 40,000 housing, health and social care professionals in England and Wales to exemplify innovative housing solutions for an ageing population.

Recognised by government and industry as a leading 'knowledge hub' on specialist housing, our online and regional networked activities:

- connect people, ideas and resources to inform and improve the range of housing choices that enable older and disabled people to live independently
- provide intelligence on latest funding, research, policy and practice developments, and
- raise the profile of specialist housing with developers, commissioners and providers to plan, design and deliver aspirational housing for an ageing population.

To access further information and resources on extra care housing, visit the Housing LIN's dedicated web pages at: www.housinglin.org.uk/Topics/browse/HousingExtraCare/

Published by

Housing Learning & Improvement Network
c/o EAC, 3rd Floor,
89 Albert Embankment
London SE1 7TP

Tel: 020 7820 8077
Email: info@housinglin.org.uk
Web: www.housinglin.org.uk
Twitter: @HousingLIN & @HousingLINews