healthwatch

Data security

A guide to keeping your data secure.

Contents

About this resource

Local Healthwatch collect, analyse and store significant amounts of data.

It's important that this data is appropriately protected to maintain public trust in the confidentiality and security of their personal information within the wider health and social care system.

Loss of this trust could affect the effectiveness of the Healthwatch network and in the wider health and social care sector.

Data security measures are designed to protect information from a wide range of threats to ensure that our information is appropriately secure, accurate and available when we need it.

This resource provides an overview of the steps you can take to keep the data you store secure.

If you have any questions, please contact research@healthwatch.co.uk.

Data security measures

- **Confidentiality**- ensuring only those who ought to have access can do so
- **Integrity-** ensuring that information cannot be modified without detection
- **Availability** -ensuring that information can be accessed when needed

Data can exist in many forms. It can be printed, handwritten, stored electronically or as digital images. The information may be transmitted by post or electronically.

Data security is achieved by using a range of controls including; legislation, policies, practices, procedures, organisational structures and software/technical controls.

Data security legislation

- Data Protection Act
- Computer Misuse Act
- Freedom of Information Act
- Public Records Act.

Data security guidance

Staff are under a common law obligation to preserve the confidentiality of service user data. Data security is everyone's responsibility and will only be successful with the active participation of all Healthwatch staff.

A data security policy is essential to keep your information secure and goes hand in hand with your data protection policy. When developing your data security policy there are several areas that you need to consider, including:

- passwords
- physical security
- emails and encryption
- social media

- unsolicited communications
- bring your own device (where applicable)
- online storage (i.e. the cloud)
- back-ups
- good practice
- only keep what's necessary
- compliance with government approved scheme (e.g. Cyber Essentials)
- IT contractors – still your responsibility as a data controller
- incident reporting

Good practice

A good data security policy will help you to make sure you address any risks in a consistent way.

You need to consider what actions you should put in place should you suffer a data breach. Good risk management can reduce the damage and distress caused to individuals by a breach.

You should always make sure that you are compliant with the Data Protection Act and any other guidelines in place. It is a good idea to document the controls you have in place and, if necessary, identify where you need to make improvements.

Consider the risks for each type of personal data you hold and how you would manage a data breach: this way you can reduce the impact if the worst was to happen.

You should also have an acceptable-use policy and training materials for staff and volunteers so that they know their data protection and security responsibilities.

Passwords

It is recommended that a password management policy is implemented by all local Healthwatch to ensure that only authorised users can access any storage systems.

All password management policies should provide guidelines on:

- how frequently people must change their passwords
- whether or not password expiry periods are enforced
- the circumstances in which passwords must be changed

This should not just cover your computer logins, but also other applications such as your CRM.

Passwords should be least 12 characters and use combination of at least 3 of the following: lower case, upper case, numbers and special characters.

Antivirus software

Antivirus software is a program designed to prevent, detect and remove software and other viruses (ie ransomware), and should be installed on all devices.

A computer without antivirus software installed will be infected within minutes of connecting to the internet.

If it is not already installed, malware/antivirus software should be installed on all devices. Malware (malicious software) is an ever-increasing problem, and there is now the added risk of ransomware, whereby cyber criminals encrypt your data and only provide you with the means to decrypt it after payment of a ransom. Data security guidance

Physical security

How and where your devices are stored is important to consider. The physical security of equipment is important to consider as devices containing personal data could be stolen in a break-in or lost whilst away from the office. You should ensure that personal data on your systems is protected against this type of threats.

You can also prevent or limit the severity of data breaches by separating or limiting access between your network components. For example, if you can confine the processing of personal data to a specific section of your network you may be able to reduce the scope of the required security measures.

You also need to ensure that the same level of security is applied to personal data on devices being used away from the office. Many data breaches arise from the theft or loss of a device (e.g. laptop, mobile phone or USB drive) but you should also consider the security surrounding any data you send by email or post.

Email and encryption

Personal and sensitive information should not be contained within the body of emails being sent outside of the trusted local Healthwatch environment.

If you do need to send this kind of information outside the organisation, it needs to be encrypted within an attachment (providing you are allowed to send it under the terms of the Data Protection Act)

What is encryption?

Encryption is a way of making sure that data can only be accessed by people with permission to do so. Typically, a strong password is required to unlock the data.

Encryption comes in many different forms and offers protection under different circumstances:

- full disk encryption means that all the data on the computer is encrypted
- file encryption means that individual files can be encrypted
- some software offers password protection to stop people making changes to the data but this may not stop an unauthorised individual reading the data.

Social media

Social media is a valuable communications tool used increasingly by the local Healthwatch network.

Social media can increase public awareness and understanding of our role, inform stakeholders and provide engagement opportunities.

However, what is published on social media may be in the public domain for a long time and information received through social media must be treated in the same way all other information would be.

- personal and private use of social media should not contain local Healthwatch information whether considered sensitive or not.
- you should not publish any confidential personal information (CPI) on any posts or through social media conversations, i.e. Yammer.

Unsolicited communications

Phishing emails continue to be a common way of deliberately delivering malicious software or viruses.

This type of attack has caused significant security and IT issues elsewhere in the public sector, including in health and social care.

Things you need to look out for:

- **Check the sender** Emails may not always be sent from the person they appear to be from, as it is possible to change the 'From' address to a name you may recognise. \

  When replying to emails, particularly those requesting information, ensure that your reply is going to the person you intend to send it to. If in doubt, speak to your manager immediately.
- **Treat links with caution** Hyperlinks in emails can often take you to fake sites or download and install viruses when clicked.
- **Avoid downloading attachments or images** Attachments may contain viruses or spyware that download to your machine when you open the file.

Using your own device for work

For organisations that allow their employees to bring their own devices (laptops, tablets and mobiles) and access sensitive personal data from these devices, it's recommended you have a Bring Your Own Device (BYOD) policy.

Using your own personal devices raises a number of data protection concerns as the device is owned by the user rather than the data controller.

Blurring of personal and business use can be a key problem. For example, people often agree to terms and conditions without really reading what they are giving external companies access to on their laptops/phones.

In addition, allowing untrusted devices to connect to your network or using work devices on untrusted networks outside your office can put data at risk.

The security of data is therefore a significant concern given that you may have a large number and a wide range of devices to consider.

Before agreeing that staff can use their own devices, the data controller will need to assess:

- what type of data is held
- where data may be stored
- how it is transferred
- potential for data leakage
- blurring of personal and business use
- the device's security capacities
- what to do if the person who owns the device leaves their employment
- how to deal with the loss, theft, failure and support of a device.

Read the Information Commissioner's Office (ICO) policy on bringing your own device: *https://www.gov.uk/government/publications/byod-guidance-executive-summary/byod-guidance-executive-summary Using online storage*

Using online storage

There are a wide range of online services, many incorporated within today's devices such as OneDrive, that require users to transfer data to remote computing facilities – commonly known as the Cloud.

Processing data in the Cloud represents a risk because the personal data for which you are responsible will leave your network and be processed in those systems managed by your Cloud provider. You therefore need to assess the security measure that the Cloud provider has in place to ensure that they are appropriate.

You should also check to see where your data is being stored. Under Principle 8 of the Data Protection Act you cannot keep it in any other countries except the European Economic Area and other ones specified. Many companies keep data stored in the USA, which is not considered safe and therefore would be a breach of the Data Protection Act.

You will need to check whether the company you're using has backup or sync switched on by default so you don't accidently end up storing data illegally overseas.

Backing up your data

If you were to suffer a disaster such as fire, flood or theft you need to be able to get back up and running as quickly as possible. Loss of data is also a breach of Data Protection Act.

You need to have a robust data backup strategy in place to protect against disasters. Backups should not be stored in a way that makes them permanently visible to another organisation, and at least one should be off-site.

Keeping what's necessary

The Data Protection Act says that personal data should be accurate, up-to-date and kept for no longer than is necessary. This means that you must have a sound reason for keeping information and once you no longer need it you should securely erase and destroy it. Data security guidance

Any data that you need to keep for statistical or historical purposes but do not need to access regularly should be moved to a more secure location. This will help prevent unauthorised access. This includes data you collect from any sources, whether stored electronically or in hard copy.

Any data, whether held on computer systems or on paper, should be subject to a strict retention schedule. We have produced a template retention and record keeping schedule that you can use as a guide when creating your own.

Whenever the retention schedule is used, the guidelines below should be followed:

- local Healthwatch requirements should be considered before deciding on retention periods
- decisions should also be considered in the light of the need to preserve records, and whether the records might be needed in the future
- retention periods should be calculated from the end of the calendar or accounting year
- the provisions of the Data Protection Act must always be followed

Working with third party suppliers

Many organisations outsource some or all their IT requirements to a third party. When doing this you should be satisfied that they are treating your data with at least the same level of security as you would. As a data controller, you are responsible for the data you have collected even when other companies are dealing with it in any way.

You should ensure that you have regular security audits of the systems containing your data as this may help to identify any risks that need to be addressed. The contracts that you have in place with your supplier must be in writing and must require them to act only on your instructions and comply with certain obligations of the Data Protection Act.

If you use a third-party supplier to erase data/dispose of/ recycle your IT equipment, make sure they do it adequately and ensure that they provide you with a certificate of destruction. You could be held responsible if personal data gathered by you is extracted from your old IT equipment when it is resold. Cyber Essentials

Cyber Essentials

Cyber Essentials is a new Government backed scheme to help organisations protect themselves against cyber threats.

Cyber Essentials defines a set of controls which will provide organisations with basic protection from the most common threats from the Internet.

It focuses on threats which require low levels of attacker skill and are widely available online.

Risk management is the fundamental starting point for organisations to act to protect their information. However, given the nature of the threat, the government believes that action should begin with a core set of security controls which all organisations should implement.

Achieving Cyber Essentials certification

To achieve accreditation, a self-assessment questionnaire needs to be completed and then reviewed by an accredited body. A pass will only be awarded if all five controls are successfully passed.

- **Secure Configuration:** To ensure secure configuration, certain steps are necessary, for example removing unnecessary software and changing the administrator password. An approved software policy should be put in place and followed by all staff.
- **Boundary firewalls and internet gateways:** This is the first line of defence between the internet and your systems. A firewall should be installed on your network, configured to block unrequired network traffic and for staff to be able to work on devices remotely.
- **User access controls and administrative privilege management:** Users should only have the amount of access that they actually need, and this should be reviewed regularly. There should be a limited number of administrator accounts, and a password policy put in place in accordance with Healthwatch England guidance.
- **Patch management:** Cyber security risks can be reduced by 80% with regular patch management. This involves updating software whenever necessary and only installing approved software. It is also feasible that installing a managed patch management service may prove the most cost-effective solution.
- **Malware protection:** If it is not already installed, malware/antivirus software should be installed on all devices. Malware is an ever-increasing problem, and there is now the added risk of ransomware, whereby cyber criminals encrypt your data and only provide you with the means to decrypt it after payment of a ransom.

Once you have passed the Cyber Essentials self-assessment, you will then need to pass an external vulnerability test by a CREST approved company.

CREST will then provide a report, highlighting any high and medium risks and how these can be mitigated. If you pass the assessment, you will receive a certificate and you can then add the Cyber Essentials symbol to your websites and documentation.

Find out more information about the Cyber Essentials here: https://www.cyberaware.gov.uk/cyberessentials/ Reporting any problems

Reporting any problems

If something does go wrong or you think that there may have been a data breach, you must report it straight away to the local authority or provider who contracts you to provide local Healthwatch activities.

They will then follow their protocol as to whether it should be reported to the Information Commissioners Office (ICO).

You should also tell us as soon as possible by emailing research@healthwatch.co.uk.

Summary

Data breaches are caused by people, processes and technology, either separately or a combination of all three.

Data security is vital for the work we do. To ensure data security remains a key issue, we're encouraging you to embrace the following principles:

- Ensure staff are equipped with the knowledge to handle information respectfully and safely
- Ensure the organisation proactively prevents data security breaches and responds appropriately to incidents or near misses
- Ensure technology is secure and up-to-date.

People have a right to expect that the information they share with you will be respected and treated appropriately. Loss of this trust may significantly impact upon the effectiveness of the Healthwatch network.

If you have any questions about data security, contact our research team research@healthwatch.co.uk. Case study