Disposal of Sensitive Information

Paper

- Staff should continuously review any paper they hold and dispose of waste paper immediately by the appropriate means.
- Staff should avoid allowing confidential waste paper to build up, by shredding confidential waste paper regularly.
- If using confidential waste bags, lock the bags away in a secure location before shredding.
- Where information is extremely sensitive it should be shredded immediately using a 'Chip' or 'Confetti' shredder.
- Never dispose of any sensitive information via normal Practice waste bins.

Electronic

- All removable media e.g. USB keys, floppy disks, laptops or desktops etc. which are broken/faulty, and have at any time contained Practice information must be permanently and verifiably destroyed.
- **Do not** donate/sell or give away computer equipment or other electronic media that your Practice no longer uses as it will still contain Practice information, even if you have deleted it.

As a business, much of the good will shown by your patients/clients is based on good relationships built up over many years. A data loss, as well as drawing negative scrutiny onto the business, can cause significant and serious reputational damage and may cause harm and distress to your patients/clients.

This leaflet is aimed at providing practical advice, tips and guidance on how you might enhance your current practices to avoid a data loss, and protect you, your business and your patients/clients data.

Tips

- Do not blur the lines between work and private life. Discussing Practice information in work does not allow you to discuss it outside of work.
- Treat all data as if it were your own personal data.
- Keep good quality factual records and keep them secure.
- Guard against people seeking information by deception.
- Identify clear lines of responsibility within your team for records and office security.
- Put Information Security on your Team Meeting agendas as a regular item.
- If you lock a cabinet or desk drawer, do not leave the key in an obvious place, such as a desk tidy.
- Remember you are responsible for the information you hold and use so protect yourself by protecting information.

Practice Policies supported by this guide

Data Protection Policy (how you comply with the Act and how Patients can access their information)

Freedom of Information Policy (how to access Practice information)

Records Management Policy (how records systems within the Practice are to be operated, and how long records are kept)

Social Media Policy (what is expected of staff when posting or using social media such as Facebook)

I.T. Security Policy (how you protect electronic equipment and information held in electronic format e.g. password policy, email policy. '*Dos and Don'ts*')

HSC Health and Social Care Board

Good Practice Guidance

Information Security

Note: all information contained within this guide correct at the time of issue: April 2013 Version 1.0 Primary Care Pharmacy

Introduction to Information Security

Information is a key asset to an organisation and it needs to be suitably protected. Information Security measures are designed to protect information from a wide range of threats in order to ensure business continuity and minimise damage. Information can exist in many forms. It can be printed or written on paper, stored electronically, transmitted by post or using electronic means (e.g. email). Whatever form information may take, or means by which it is shared or stored, it should always be appropriately protected. Failure to protect information assets can result in significant harm being caused to both the controller of the information, and in the event that personal information is not protected, the person to which the information relates. Information Security can be defined as a set of processes, policies, measures and practices that work together to protect the **C**onfidentiality, **I**ntegrity and **A**vailability of data and information.

Confidentiality – Access to information is confined only to those with the authority to view that data. (*Access protocols will mitigate risk of loss or unauthorised access*.)

Integrity – Safeguarding the accuracy and completeness of information by protecting against unauthorised changes or deletions, whether deliberate or accidental. (*Electronic measures and physical controls/version controls mitigate this risk*.)

Availability – Information is delivered in a controlled fashion to the right person, when it is needed. (*Having robust and accessible records management processes and systems which monitor access will facilitate this*.)

> **Fact:**
>
> Since 2011 the ICO has had the powers to fine organisations up to **£500,000** for serious data breaches.
>
> **Source: Information Commissioners Office**

Practical Advice

- Operate a 'Clear Desk Policy'. Remove or secure information within the work area and lock your computer screen during breaks, periods of leave or when the Practice is closed each evening and at weekends.
- Keep filing cabinets and cupboards closed and locked. Do not leave keys in their locks.
- Use a tracer card to monitor authorised access to sensitive hard copy documents.
- If you need to upgrade, repair or access secure storage to hold information, bring this to the Manager's attention.
- Identify all sensitive information you hold in whatever format, and assess the current measures used to secure it/protect it.
- Paper and computer media should be stored in lockable cabinets/drawers when not in use, especially outside working hours.
- Sensitive information must be locked away (ideally in a fire-resistant safe or cabinet) when not being used.
- Your workstation should be positioned in such a way that prevents others, including patients, from viewing sensitive information either on your desk or your PC screen.
- Consider restricting the use of Smart Phones to tea/dinner breaks and do not permit photos or videos to be taken on the premises as this may inadvertently capture patient data.
- Notify your Manager immediately if work keys or sensitive documents are missing.
- To ensure the security of information held electronically always lock away portable devices such as Laptops when not in use.
- If your work requires you to use a USB key to transfer information, ensure that it is sufficiently encrypted (256-bit or above).
- Limit the amount of personal information you hold. If you do not need personal data to carry out a task, use anonymised data.

Password Security

Your password is your main protection against someone else using your account and it acts as a barrier against someone else accessing sensitive information in your possession.

What you should do:

- Have a Practice policy of changing your password regularly.
- Add some numbers to your password.
- Try to add characters such as £ * ^ % etc. into your password.
- Always keep your password secret.
- Change your password immediately if you suspect someone knows it, and inform your line manager.
- Log out or lock the computer when it is unattended e.g. during tea or lunch breaks. **(Press the Windows Logo Key + L)**

What you should NEVER do:

- **Do not** create a password that is easily guessed, avoiding such information as car registrations, date of birth, names of people or pets etc.
- **Do not** share passwords or system accounts. If a person needs access to something held on another staff members machine, they must speak to their Line Manager to gain permission.
- **Do not** write down passwords and stick them to computers or keep it in a drawer.

Internet Based Email accounts

The Health and Social Care Board **does not recommend** the use of free internet based email accounts for use as a business tool for the transfer of sensitive information. These type of accounts are more prone to being compromised and therefore increase your risk of suffering a data loss. Examples of free internet based email accounts include Hotmail, Yahoo, Gmail etc.