PARK VIEW GROUP PRACTICE

**2 Longford Road West, Reddish, Stockport SK5 6ET**
**Tel: 0161 426 9500 Fax: 0161 431 5140**
**www.parkviewgrouppractice.co.uk**

# Data Security Policy

| Document Control | |
|---|---|
| **Document Name** | Data Security Policy |
| **Publication Date** | August 2018 |
| **Version Number** | 1.0 |
| **Target Audience** | Practice Staff |
| **Description** | To ensure Park View Group Practice is compliant with data security and the law |
| **Action Required** | To Note |
| **Author** | Amy Waters |
| **Next Review Date** | August 2019 |

# Contents

## Introduction

With the implementation of GDPR and the new NHS IG Toolkit, it is important for staff to be more vigilant with regards to data security standards, types of information, the law, threats to data security and how to avoid breaches. This policy explains how to ensure good practice to avoid data breaches and cyber incidents.

## NDG Data Security Standards

Below are the ten security standards Park View Group Practice needs to comply with:

1. All staff must ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is only shared for lawful and appropriate purposes.

2. All staff must understand their responsibilities under the National Guardians data security standards including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.

3. All staff must complete appropriate annual data security training and pass a mandatory test, provided through the revised Information Governance Toolkit.

4. Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access to personal confidential data on IT systems can be attributed to individuals.

5. Processes are reviewed at least annually to identify and improve procedures which have caused breaches of near misses, or that force staff to use workarounds which compromise data security.

6. Cyber-attacks against services are identified and resisted and CareCERT security advice is responded to. Action is taken immediately following a data breach or a near miss, with a report made to senior management within 12 hours of detection.

7. A continuity plan is in place to respond to threats to data security, including significant breaches or near misses. As a minimum, it is tested once a year, with a report made to senior management.

8. No unsupported operating systems, software or internet browsers are used within the IT estate.

9. A strategy is in place for protecting IT systems from cyber threats. This is based on a proven cyber security framework, such as Cyber Essentials, this is reviewed at least annually.

10. Suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardians data security standard.

## Types of Information

It is important to comply with the law to protect personal information, because health and care information is valuable. Poor security can cause personal, social and reputational damage:
Losing information – including paper records via fax and by losing computers or mobile phones – or disclosing information over the phone.
Theft of information – such a clicking links to fake websites.
Insecure storage – and disposal of information leading to loss or theft.

In health and care settings, we come into contact with various types of personal information about people. It is important to identify different types of information so that they can be appropriately protected when they are used and shared:

***Personal information*** – information about someone is 'personal' when it identifies an individual. It may be about living or deceased people, including patients, service users and members of staff.

You may also come across the term 'personal data' which is used in the Data Protection Act 2018 and is a subset of personal information. Some personal data may be 'sensitive personal data' because it concerns a person's health and care.

A person's name and address are clearly information when presented together, but an unusual name may, by itself, enable an individual to be identified.

Personal information may be recorded in hard copy or digital for e.g. photographs, videos and DVS, whiteboards, health and care records, personnel files and on a computer – or it may be information simply know by others (such as the care team).

***Confidential information*** – confidential information is information that patients and service users disclose in confident to staff who are providing their health and care – they expect that information to be treated confidentially.

It can include names and addresses, as well as a person's sensitive information – for example, health and care information.

Third party information, such as family details, added to a patient or service users notes, should also remain confidential.

As mentioned previously, all health and care information is sensitive, but patients and service users may consider particular types of information to be highly sensitive e.g. information relating to their mental or sexual health.

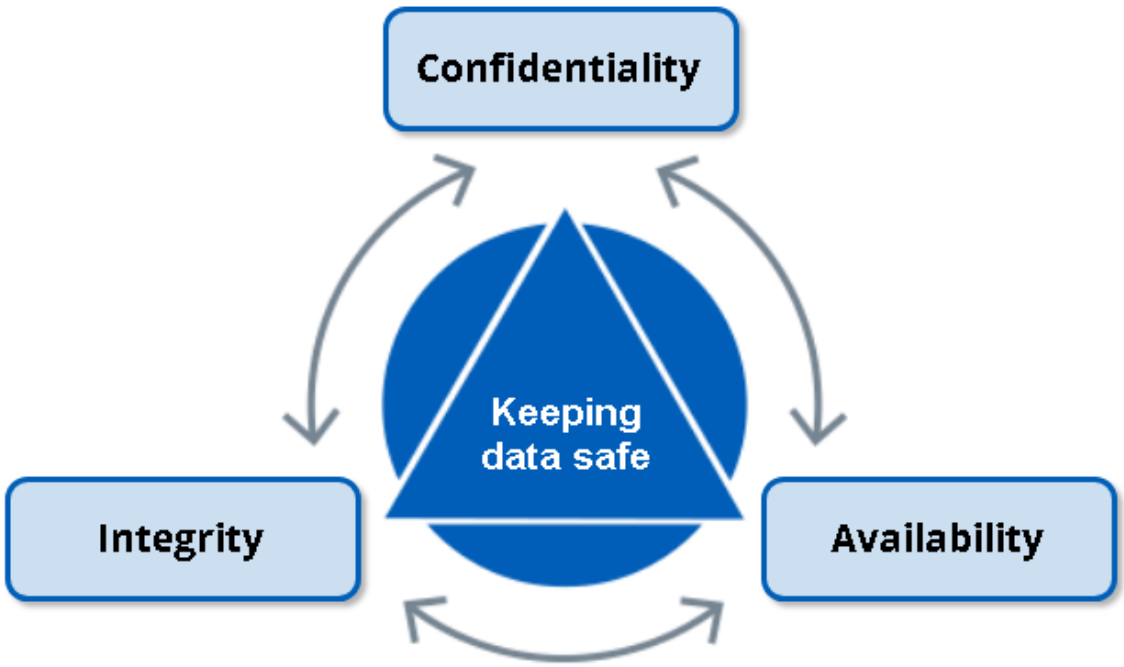
***Anonymised information*** – this information does not identify an individual and cannot reasonable be used to determine their identity. Anonymisation requires the removal of name, address, fill postcode and any other detail or combination of details that might support identification.

Anonymised information does not identify a person, so it cannot be personal or confidential.

***Pseudonymised information*** – is information in which individuals are distinguished by using a unique identifier (that is, a pseudonym). This does not reveal their 'real-world' identity, but allows the linking of different data sets for the individual concerned.

## Data Security can be broken down into three areas:

**Confidentiality, Integrity and Availability:**



***Confidentiality*** – is about privacy and ensuring that information is only accessible to those who have a proven need to see it. It would be unacceptable for a perfect stranger to be able to access sensitive information from a laptop simply by lifting the lid and switching it on. That's why a laptop should be password protected and the data on it encrypted when switched off.

***Integrity*** – is about information being accurate and up to date. Systems must be designed so that the input and management of information not prone to human error that the flow of information does not result in loss or alteration.

***Availability*** – is about information being there when it's needed to support care. System design must include appropriate access controls and checks, so that the information in the system has consistency, accuracy, can be trusted as correct and can be relied on when providing health or care.

# Introduction to the Law

## *What is confidentiality?*

The focus of confidentiality is consent. Under the common law duty of confidentiality, confidential information should not be used or shared further without the consent of the individual. Exceptions to the requirement for consent are rare and limited to:

- A legal reason to disclose information, for example, by Acts of Parliament or court orders
- A public interest justification for breaching confidentiality such as a serious crime.

Decisions on whether or not to breach confidentiality should be made by senior staff. For example, your IG Lead or Caldicott Guardian.

## *Caldicott Principles*

Before using confidential information, you should consider the Caldicott Principles:

1. **Justify the purpose(s) for using confidential information** – this means you should not use or share information unless you have a valid reason. For example, wanting to send a friend a birthday card is not a valid reason to access the records your organisation holds about them.
2. **Don't use confidential information unless it is absolutely necessary** – if you believe you have a valid reason, ask yourself if it is essential that you use confidential information, or can the purpose be met without identifying any individual(s)? For example, if you are asked for information about how **many** people have attended for an appointment, it would not be necessary to provide names and addresses of each person who attended.

3. **Use the minimum necessary confidential information –** If you have to use confidential information, you need to be clear on what is actually is required to meet the purpose. If a particular part of the information is not necessary, it should not be used or shared. For example, if you receive a valid request for details about a patient/service user's last attendance at your organisation, it would not be appropriate to provide the requestor with the entire record of care/treatment.
4. **Access to confidential information should be on a strict need-to-know basis** – information should only be available to authorised members of staff. You should not attempt to access information that you need to see as part of your role or to use someone else's account details. You should never allow anyone to log into systems using your details. If you intend to share the information, it should only be shared with those who need it carry out their role.
5. **Everyone with access to confidential information should be aware of their responsibilities** – you should attend the provided training and awareness session so that you understand your responsibility for protecting information. If you intend to share the information, you must ensure that the recipient is aware of their responsibility for protecting the information – and of the restrictions on sharing it further.
6. **Understand and comply with the law** – when you use confidential information, there is a range of legal obligations for you to consider. The key obligations are outlined in the Common Law Duty of Confidentiality and un the Data Protection Act 2018. If you have a query about the disclosure of confidential information, you should contact the Practice Manager if you are still not sure.
7. **The duty to share information can be as important as the duty to protect confidentiality** - You should have the confidence to share information in the best interests of your patients and service users within the framework set out by these principles. The practice will support you by providing policies, procedures and training.

## *Confidentiality – good practice*

We all have a legal duty to respect the privacy of our patients and service users, and to use their personal information appropriately.

The main aspects of good practice in the area of confidentiality are:

- Informing people
- Sharing information for care
- Sharing information for non-care

### Informing people

Patients and service users will not expect health and care professionals to look at their health record unless those professionals are involved in their care. Wherever

possible, you should inform patients and service users that you are accessing and using their information, and the reason for doing so.

The Practice clearly explain to patients how we will use their personal information through the Fair Processing Notice, which is available in leaflet format and on the Practice Website.

Patients are given a choice about how their information is used and the Practice will tell them if their choice will affect the services offered to them. For example, it may not be possible to provide some services without being able to access their information.

The Practice wants to meet expectations by only using personal information in ways that patients would reasonably expect.

### Sharing information for care purposes

Sharing information with the right people can be just as important as not disclosing to the wrong person.

You have a legal duty to share the information:

- If it will assist in the care or treatment of an individual, AND
- It is reasonable to believe that the individual understands the reason for sharing.

Practice staff will ensure:

- the patient understands what information will be shared and has no concerns
- data protection, record-keeping and security best practices are met
- respect individual patient objections to any proposed information sharing, you must respect their objection even if it undermines or prevents care provision

### Sharing information for non-care purposes

In many cases, consent should be obtained if you want to use someone's personal information for non-care purposes, such as commissioning and research.

However, if there is a risk of immediate harm to the patient or service user, or to someone else – and you cannot find an appropriate person with whom to discuss the information request – you should share the information.

If the request from the Police, please ask them to complete the appropriate form.

At the first opportunity after, you should inform the person responsible for Information Governance in your organisation so they can follow up the legal basis for sharing.

## *Data Protection Act 2018 & General Data Protection Regulations 2016*

The Act provides people with several rights, the most relevant of which, in a health and care setting, are:

- The right to be informed about what their personal information is being used for and who it may be shared with (fair processing notice)
- To have objections to their information being processed considered where they claim they are suffering unwarranted distress or damage as a result
- To see and have a copy of their information (subject to access)
- To have an objection to the use and sharing of information held in confidence. Objections should be respected, unless there are exceptional reasons to the contrary

## *Rights of Individuals*

Patients and service users currently have the right to:

- Make subject access requests (SAR)
- Have inaccuracies corrected
- Have inaccurate personal data rectified, blocked, erased or destroyed in certain circumstances
- Object to direct marketing
- Restrict the processing of their information, including by automated decision making systems or programmes.

In addition to accurately recording facts, we must consider that the patient might be able to view their record online.

When providing people with access, care must be taken not to reveal information that they do not already know relating to third parties. For example, information in their record about family members, this information is redacted from the online medical record.

## *Data Protection – good practice*

Certain simple actions can ensure that you comply with the principles of the Data Protection Act:

- Handle personal information only in ways in which the individual would reasonably expect. Be open, honest and clear. **THINK: how would you expect others to handle your personal information?**
- It is important that records are full, accurate, dated and timed. The should distinguish between clinical or care findings, your opinions and any other information provided by others. This is particularly applicable to making decisions about a child's or young person's safety or welfare.
- Stick to the Practice rules for the disposal of personal information. Seek advice from the IT Administrator when disposing of information held on digital assets. All devices such as laptops must be disposed of by GMSCU.

### *Freedom of Information Act 2000*

Where an organisation uses public money, the Freedom of Information Act 2000 puts duty on the organisation to provide information to individuals who make a written request for it.

Members of the public can make Freedom of Information (FOI) requests in three ways: by letter, by fax or by email. An FOI request cannot be made verbally.

The FOI Act 2000 allows anyone from anywhere in the world to ask for information held by the Practice.

Individuals don't need to say who they are (other than to provide adequate correspondence details) or why they want the information. The information must be provided, even if it presents the organisation in a poor light.

The Act only applies to information that already exists in a recorded form (for example, documents, emails, written notes and tape recordings). It does not normally required an organisation to create new information in order to meet a request.

Handling FOI requests is a technical skill that should be dealt with by trained staff.

You should not try to handle a request yourself unless you have been trained to do so.

Park View Group Practice is subject to the Freedom of Information Act, you do have some responsibilities:

1. Make sure you know who is responsible for managing requests, which is the Practice Manager or Data Co-ordinator
2. Send any FOI requests you receive to the person responsible as soon as possible, to comply with the turnaround time of 20 working days.

**All FOI requests must be responded to within 20 working days.**

## Record Keeping – good practice

Poor-quality information presents a risk to patients, service users, staff members and the Practice. If you are uncertain about any of the good practice raised in this section please speak to the Practice Manager.

To ensure records are accurate and up to date:

- Make sure that you know what needs to be included in the record, why you are recording the information and how it will be used. The information that you enter must be correct and clear.
- Make sure you record the information on the correct system and in the correct record.
- Give individuals the opportunity to check information about themselves and point out any mistakes or inaccuracies.
- If you are not a health or care professional, you should check the information with someone who is, or cross-reference the information with other records.
- Follow the Practices process to report and correct errors.
- When using shared records, ensure that they are kept up to date so that other providers have the correct information available to them.
- Record information while the event, care or otherwise is still fresh in your mind.
- Include the NHS number in health and care records (this helps to ensure that the correct record is accessed or shared for the correct patient)
- Before you create a new record, make sure that one doesn't already exist, so the record is free from duplication
- Save records in a secure place that is easy to find.
- Ensure that records are stored safely and securely, and can be quickly located when required.

We all have a responsibility to use information lawfully. To make sure you comply with the law, you must know and comply with any Data Protection Act and/or Freedom of Information Act that the Practice has in place.

Sharing information can improve the speed and quality of service that we provide to the public, so don't be afraid to share information on a need-to-know basis.

Make sure that it is shared in a secure way and that you have consent to do so. Give individuals an opportunity to check the accuracy of information and records held to enable any mistakes to be corrected.

If you are unsure, you should ask for help, or seek advice from those who are responsible for information governance at the Practice.

# Threats to Data Security and How to Avoid Them

## *Social Engineering*

Social engineering involves those who want to steal data, such as health and care records – either digital or physical – by using tricks or deception to manipulate people into giving access to that data and other valuable information.

Criminals will often take weeks and months getting to know a place before even coming through the door or making a phone call.

Their preparation might include finding the Practices phone list or chart and researching employees on social networking sites like LinkedIn or Facebook.

The goal is always to gain the trust of one or more employees, through a variety of means.

**Examples of Social Engineering:**

- They might call and pretend to be a fellow employee e.g. GMSCU or a trusted outside provide like the Police.
- Criminals posing as a Facebook "Friend" – however, you can never be certain that the individual you are talking to on Facebook is a real person. Criminals are stealing passwords, hacking accounts and posing as friends for financial gain.

## *Using email safely*

Email can be the most efficient option for exchanging information securely but, as with all forms of information transfer, there are risks.

Hackers and criminals sometimes use unsolicited emails that contain attachments or links to try to trick people into providing access to information. This type of threat is known as phishing.

If you receive a request from a supposed colleague asking for login details or sensitive, financial or patient/service user information, you should always double-check the request with that colleague over the phone.

Equally, if you receive an unsolicited email that contains attachments or links that you have not asked for, do not open them.

Remain vigilant and report the suspicious email to your IT Administrator or GMSCU.

**Never give your login details to anyone.**

## *Phishing*

Phishing is by far the biggest and easiest form of social engineering.

Criminals use phishing emails and websites to scam people on a regular basis. They are hoping that you will click on fake links to sites or open attachments so that they can steal data or install malicious software.

The aim of phishing emails is to force users to make a mistake – for example, by imitating a legitimate company's emails or by creating a time-limited or pressurised situation.

Phishing email attachments or websites might ask you to enter personal information or a password, or they could start downloading and installing malware.

Be vigilant:

1. Do not install any new software unless you are advised to do so by the GMSCU or Practice IT Administrator
2. Think – is someone trying to extract or extort information from you?
3. If you are unsure, or think that this may be happening to you, contact the IT Administrator and GMSCU immediately
4. If you have clicked on a phishing link or visited a phishing website, contact the IT Administrator or GMSCU immediately for advice.

### What to do?

What do you do if you receive a phishing email?

1. Do not reply
2. Select the email, right click it and mark it as junk
3. Inform your IT Administrator or GMSCU and they will advise on how you can block further emails being received

## *Macros*

Macros are a series of actions that a programme such as Microsoft Excel may perform to work out some formulas. Your computer will disable macros by default because they can be programmed to install malware. Always be vigilant when enabling macros. Do you trust the source of the document?

## *Malware*

Malicious software (malware) can reside on your computer and evade detection, making it easier for someone to be active on your system without you noticing.

To protect the Practice from this type of threat, the GMSCU ensures that we have up-to-date antivirus software installed.

Malware can make computers run slowly or perform in unusual ways. If you suspect that your computer is not performing as it normally does, contact your IT Administrator or GMSCU.

## *Untrusted Websites*

Be vigilant when you visit a website that is declared 'untrusted'. If a web browser states that you are about to enter an untrusted site, be very careful: it could be a fake phishing website that has been made to look genuine. A browser may display a red padlock or a warning message stating your connection is not private.

## *Good Practice - Passwords*

It is important to use strong passwords on all of your devices to prevent unauthorised access. You should also use different passwords on each account. Creating strong passwords doesn't need to be a daunting task if you follow some simple guidelines. For more help managing and setting passwords please view the following guidance:

https://www.ncsc.gov.uk/blog-post/three-random-words-or-thinkrandom-0

You should lock your device as soon as you stop using it. ALL mobile phones, laptops, PCs and tablets, whether personal or not, should have a passcode set. If you see a colleagues device open and unlocked, lock it for them and gently remind them to do so in the future.

To lock a computer press the Windows Key plus the L Key on your keyboard.

Do not use unauthorised USB drives and avoid plugging in any non-approved devices to charge via a USB cable. A private mobile is effectively a removable device/drive and may contain malware.

Before using a USB device/drive you should scan it to ensure it is safe and virus free.

If you are permitted to use other USB drives, you should never plug a non-secure USB drive into your work computer as this could introduce malware or viruses onto your computer and then onto the Practices network.

Similarly, you should never plug a secure USB drive into an untrusted computer.

## *Disposal of confidential information*

We have to be careful when disposing of any information. Much data that health and care organisations create and use is classed as official in the eyes of the government.

The government defines 'official' as the majority of information that is created or processed by the public sector. This includes routine business operations and services, some of which could have damaging consequences if lost, stole or published in the media.

### *Good Practice – physical security*

There are some simple steps that we can take to increase the physical security of the Practice:

1. Shut or lock doors and cabinets as required
2. Maintain a clear desk policy when away from your desk
3. Wear your name badge
4. Query the status of strangers (if it is safe to do so), especially if they try to follow people into staff areas
5. Know who to tell if anything suspicious or worrying is noted
6. Don't tell unauthorised personnel how the security or other business-sensitive systems work
7. Know what an incident or breach is in the Practice – and know when to report one.

## Clear Desks

Please be aware the Practice has a clear desk policy that must be adhered to. The purpose of this policy is to:

- Ensure that you are not potentially leaving sensitive information lying around, raising the risk of a breach
- Reduces the risk of data loss by ensuring no confidential or commercial information is left unattended throughout the workplace
- Not leave information – such as documents that identify someone or financial details – in unsecure locations

## Breaches and Incidents

In the Practice, you must be able to spot common activities where information could be lost, stole or compromised and know what to report. All members of staff provide our first line of defence against information loss and theft.

You should be aware of the several ways in which data security might be compromised. However it is important to understand that such incidents typically fall into two categories:

**Breaches** – a breach of one of the principles of the Data Protection Act and/or confidentiality law

**Cyber incidents** – a technology-related incident

You have a responsibility to know how to report data security incidents:

- If you know or suspect that a data security incident has taken place, register it in line with the Practices incident reporting procedure
- 'Near misses', where data was nearly lost or where there was nearly a breach, should also be reported
- Report the data security incident to the Practice Manager as soon as possible. That way they can assess how serious the incident is and start an investigation.
- Know the Practices Fair Use of ICT policy
- Do not alter or change any software on your device without permission

## *How to avoid postal breaches*

1. Make sure that all correspondence containing personal information is always addressed to the named person
2. If the letter contains more than basic clinical information, consider sending it recorded delivery
3. Make sure there are no other patients letters in the envelope accidentally

## *How to avoid email breaches*

1. Ensure it is acceptable to send personal information in this way
2. Confirm the accuracy of the email addresses for all intended recipients, sending test emails if you are unsure
3. Check that everyone on the copy list has a genuine 'need to know' the information you intend to send
4. When referring patients or service users, use the minimum identifiable data (i.e. their NHS number)
5. Check that the transfer is from an NHSmail account to an NHSmail account, or if you are sending sensitive information outside of NHSmail, then you should use the encryption feature. The only exception is when sending emails ending in *secure.nhs.uk.
6. To encrypt an email enter [secure] in the subject header.
7. Where an email needs to be sent to an unsecure recipient, check whether this is at the request of a service user who understands and accepts the risks. Consider whether it would be more appropriate to encrypt the email yourself.

## *How to avoid telephone breaches*

1. Confirm the name, job title, department and organisation of the person requesting the information
2. Confirm that the reason for the information is appropriate
3. Take a contact telephone number. For example, the main switchboard number – never a direct line or mobile phone number – so that you can phone back and confirm that the caller is genuine

4. Check whether the information can be provided – if in doubt, tell the person you will call them back
5. Only provide the information to the person who requested it (do not leave messages)
6. Ensure that you record your name, the reason for the disclosure and who authorised the disclosure on the record spreadsheet.

## *How to avoid fax breaches*

1. Faxing personal details separately from clinical details, with the exception of an individual's NHS number
2. Double checking the fax number and using preprogrammed numbers
3. Telephoning the recipient of the fax to let them know she is going to send confidential information.
4. Ask the recipient to acknowledge the fax
5. Make sure your fax cover sheet states who the information is for and mark it 'Private and Confidential
6. Either request a confirmation that the transmission was completed or call to confirm
7. After you have sent the fax, make sure you remove the original document from the fax machine