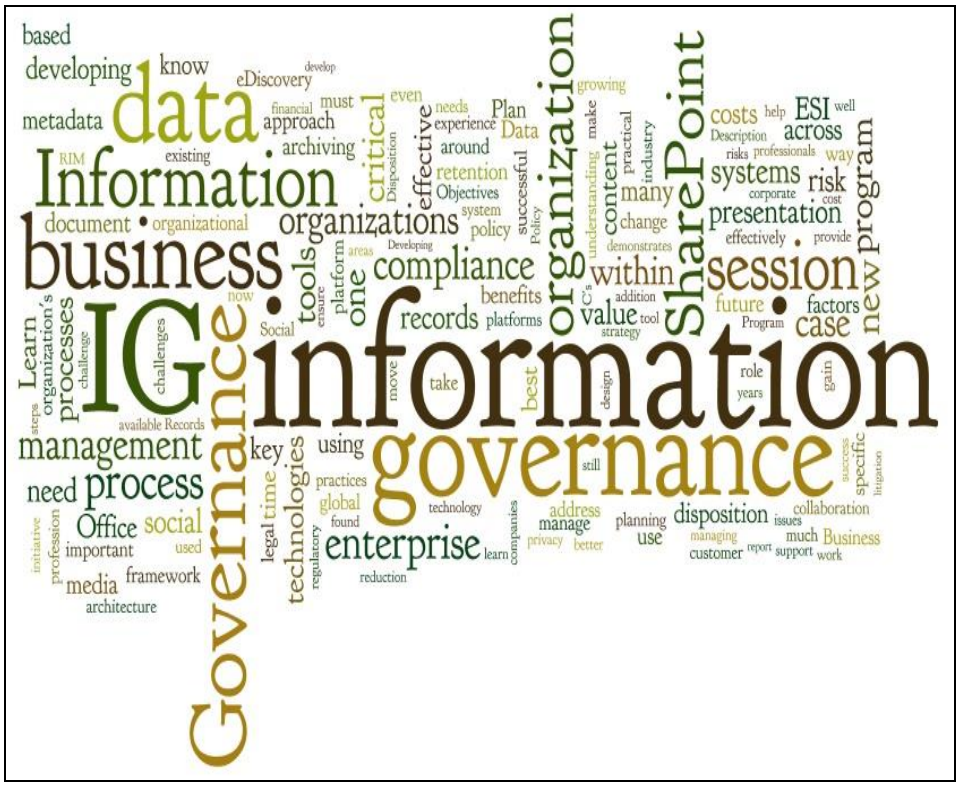
Milton Keynes University Hospital
NHS Foundation Trust

Information Governance Workbook

For All Staff (except Facilities, Estates and Volunteers)



Please ensure you read the workbook thoroughly before completing the online assessment

Learning Outcomes

You'll find out about:-

- How to avoid breaching confidentiality, law and best practice guidelines
- How to comply with Data Protection and Freedom of Information, Caldicott Principles, Best Practice and relevant legislation
- Good record keeping corporate/clinical
- Effective information security
- Good IT security

Contents

IG and You

Put simply Information Governance (IG) is a set of good practice guidance that should be followed when processing information. It allows organisations and individuals to ensure information is processed legally, securely, efficiently and effectively.

IG applies to all types of information the Trust may process, but the rules may differ according to the type of information concerned.

This booklet is designed to test your knowledge and awareness of Information Governance requirements and replaces the need to attend an Information Governance classroom based session.

Staff must read the following pages and complete the online assessment questions available on the workforce website. By completing this workbook you are making the declaration that you have understood your responsibilities under Information Governance

IG Support

All policies, procedures and guidance documents are available on the IG Intranet Pages http://nww2.mkhospital.nhs.uk/informationgovernance

IG Contacts

Dawn Budd, Information Governance Manager/Data Protection Officer	85041
Heidi Walker, Deputy Information Governance/Security Manager	85045
Jolene Neil, Information Governance Officer	85043
Ann Gibbons, Information Governance Officer/Freedom of Information	85044
Aimee Moore, Information Governance Administrator/Access to Health	85042

What is IG?

Information Governance (IG) determines the way the Trust processes or handles identifiable information about its patients and staff. It includes aspects of law such as the Data Protection Act 2018 incorporating the General Data Protection Regulation, the Freedom of Information Act 2000 and the common law of duty of confidentiality. It also incorporates national guidance from the Department of Health, such as the codes of practice on confidentiality, records management and information security.

IG covers personal information: information relating to patients/service users and employees, and corporate information such as finance and estates records.

It provides a way for Trust staff to deal consistently with the many different rules about how information is handled. This will ensure that everyone can be more confident that information is:-

- Protected by adequate security
- Only shared on a need to know basis
- Accurate and up to date
- Available as and when required

Ultimately, it means that the Trust will be able to deliver the best possible service to its patients.

REMEMBER:- breaches in confidentiality can have a monetary impact and could also result in damaging the reputation of the Trust and loss of confidence from our patients.

Why is IG so important?

The rules and procedures that make up Information Governance ensure that we provide a confidential service to our patients and they feel safe in the knowledge that they can trust us with their information.

Confidential Service

We are all responsible for Information Governance and must all, therefore, know what information is confidential and how to maintain that confidentiality.

We must ensure that information is kept secure and reported as an incident when it is not. From these reports we can then improve our work practices to prevent further incidents through shared learning.

Staff that have little or no contact with patients will still see and hear information about patients that must be kept confidential. You may see a neighbour, friend or colleague attending the hospital as a patient. This remains that individual's confidential information. Furthermore, we are all still bound by the laws of confidentiality even after we leave the workplace.

Patient Trust

Patients trust the NHS and MKUHFT to record information about their ongoing healthcare, look after that information securely and only share on a need to know basis.

SIRO and Caldicott Guardian

The Trust has appointed John Blakesley, Deputy Chief Executive as Senior Information Risk Owner (SIRO). The SIRO has lead responsibility to ensure Trust information risk is properly identified, managed and that appropriate assurance mechanisms exist. The SIRO will also advise the Trust Board on risks associated with sharing and protecting information.

In addition to the SIRO, the Caldicott Report, which was conducted in 1997, required that every NHS organisation must appoint a senior person to be responsible for protecting the confidentiality of patient information and to enable appropriate information sharing. The

Caldicott Guardian plays a key role in ensuring that the NHS, Councils with Social Services responsibilities and other partner organisations satisfy the highest practicable standards for handling patient identifiable information.
The Trust's Caldicott Guardian is Dr Ian Reckless, Medical Director.

Both the above are supported by the Information Governance Manager, Dawn Budd and her team.

Personal, Confidential and Sensitive Information

Personal Information

Information about an individual is personal when it enables an individual to be identified.

This isn't always straightforward. For example, a person's name and address are clearly personal information when presented together, but an unusual surname may itself enable someone to be identified. This is an important distinction in law.

Confidential Information

Personal information is classed as confidential if it is provided in circumstances where an individual can reasonably expect that it would be held in confidence, for example the doctor/patient relationship.

Information is considered confidential if it meets three simple conditions:

- **It is private information about a person**
- **It is provided to someone who has a duty of confidence (for example, a doctor or nurse)**
- **It is expected to be used in confidence**

Special Category Data (Sensitive Information)

Sensitive personal information is information that is more likely to cause a person damage or distress if the information were to be misused.

For example:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation.

Sharing Information and Consent?

Abuse of privilege

It is strictly forbidden for staff to knowingly browse, search for or look at any information relating to themselves, their own family, friends or colleagues without a legitimate purpose such as treating a patient. This includes accessing paper or electronic health records, test results, etc.

Action of this kind will be viewed as a **breach of confidentiality**, of Trust policy and of the Data Protection Act 2018/GDPR and dealt with under the Trust's Disciplinary Policy and may be reported to the Information Commissioner

Duty of confidence

A duty of confidence arises when sensitive information is obtained and /or recorded in circumstances where it is reasonable for the data subject of the information to expect the information will be held in confidence.

Patients provide sensitive information relating to their health and other related matters as part of their seeking treatment and they have a right to expect that we will respect their privacy and act appropriately. The duty can equally arise with some staff records, for example occupational health, financial matters etc.

Patients have a right to be informed about how we will use their information for healthcare, the choices they have about restricting the use of the information and whether exercising this choice will impact on the services offered to them. The Trust has produced a patient leaflet "Patient leaflet on guide to storing information" which gives patients information on the collection use and storage of their information. It is available in all clinical areas across the Trust. Further copies can be printed from the Trusts intranet/internet sites.

Explicit informed consent

Where it is proposed that patient information is disclosed outside of the Trust for purposes other than direct healthcare, in most cases it is necessary to ensure the patient has **explicitly consented** to this happening. For example, patient information used for research purposes.

Legal requirement

Always remember confidentiality is a legal requirement, supported by the confidentiality clause in your contract and, where applicable, your professional code of conduct.

All requests from the Police for statements, records or images should be directed to the Information Governance Team for action or out of hours Duty Manager on-call

Why protect information?

UK and European laws such as the The Data protection act 2018/GDPR, Computer Misuse Act 1990 and the Common law duty of confidence, demand it.

The Data Protection Act 2018

This Act sets out how the Trust should process and handle personal data. It also details the rights of the individual in relation to the data that is held about them. This applies to all data for held. These rules also apply to all records an employer holds about a staff member, for example finance details and personnel records.
There are six Data Protection Principles (see below) that define how organisations should look after information. Any breaches of these principles can result in legal action being taken against an individual and / or the organisation.

1. Processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')
There is a requirement to make the general public, who may use the services of the NHS, aware of why the NHS needs information about them, how this is used and to whom it may be disclosed. • There should be no surprises, so … inform patients or staff why you are collecting their information, what you are going to do with it and who you may share it with • When formulating a research project remember to be open and transparent about what you will be doing with the information and ensure correct procedures are followed and consent is obtained prior to collection • Ensure that the patient or staff member is aware of who will have access to their information, and that all those involved may need to see their notes • Be open, honest and clear
2. Processed for Specified, explicit and legitimate Purposes
Only use personal information for the purposes for which it was collected. • Personal information on a Patient Administration System must only be used for healthcare purposes by those with a legitimate reason to see it i.e caring for the patient. The system is not there for looking up your family, friends' and colleagues personal information. This is against Trust Policy and Data Protection law and could lead to disciplinary action/prosecution • Only share information outside your team, ward, department or service if you have the authority to do so and certain it is appropriate and necessary • If in doubt, check first!
3. Adequate, Relevant and limited to what is necessary
Only collect and keep information you require. It is not acceptable to hold information unless you have a view as to how it will be used. • Do not collect information "just in case it might be useful one day" • Do not take both daytime and evening telephone numbers if you will only call in the day • Explain all abbreviations • Use clear legible writing • Stick to the facts – avoid personal opinions and comments

4. Accurate and where necessary, kept up to date.

Every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay

Information must be kept accurate and up to date. Take care in- putting data, think about the steps you can take to make sure it is accurate.

- How do you know information is up-to-date?
- Each time a patient attends a clinic, they should be asked to confirm their details are correct – address, telephone numbers etc
- Check existing records thoroughly before creating new records
- Avoid creating duplicate records
- Enter in a timely manner

5 Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed

Ensure that you:-

- Follow the Trust's Retention guidelines which can be found within the Information Governance Policy, and your own departmental guidelines.
- Undertake regular housekeeping
- Dispose of information in line with Trust Policy.
- All new members of staff should familiarise themselves with this policy when they join the Trust.

The Trusts Information Governance Policy can be found on the intranet at :- Information Governance Policy

6 Processed in a manner that ensures appropriate security of the personal data including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality'

All individuals have rights with regard to their personal data as follows:-

Access to their healthcare/staff records – forms are available on the Intranet at Access to Health Records forms

Right to privacy - Ensured that your data is processes on a fair and lawful basis
Right to be informed – Processing of Personal data must be concise, transparent, intelligible and easy accessible.
Right of access - You can find out if we hold any personal information by making a 'subject access request' under the Data Protection Act 2018
Right to rectification - You are entitled to have personal data rectified if it is inaccurate or incomplete
Right to erasure (to be forgotten) - The right to erasure does not provide an absolute 'right to be forgotten'. you have a right to have personal data erased and to prevent processing in specific circumstances
Right to restrict processing – Contesting accuracy, objecting to processing and unlawful processing.
Right to data portability - allowing you to obtain and reuse your personal data for your own purposes across different services.
Right to object - You must have an objection on "grounds relating to your particular situation"
Rights to know if we carry out automated decision making and profiling

Please direct all requests to the Information Governance Office.

The Trust can be fined up to 4% of its annual turnover or 20 Million Euros (whichever is greater) Remember you can also be fined personally if you deliberately breach the Data Protection Act 2018 accessing information that you shouldn't.

This Act applies to all personal identifiable information held in manual files, computer databases, videos and other automated media, such as personnel and payroll records, medical records, other manual files, microfiche/film, pathology results, x-rays, CD's, USB Sticks etc, and anything we do with that information i.e:-

Collection	Use
Disclosure	Sharing
Destruction	Transfer

How else can you be identified?

Name	Date of Birth	DNA	Titles such as
Address	NI Number	Fingerprints	Mother
Postcode	DVLA Number	Photo	Brother
	MRN Number	Tattoos	Social Services
	NHS Number	Disability	Job Titles
		Height/ Weight	

Computer Misuse Act 1990

The Computer Misuse Act is designed to protect computer users against wilful attacks and theft of information.

Offences under the act include hacking, unauthorised access to computer systems and purposefully spreading malicious and damaging software (malware), such as viruses.

Unauthorised access to modify computers include altering software and data, changing passwords and settings to prevent others accessing the system, interfering with the normal operation of the system to its detriment.

The act makes it an offence to access or even attempt to access a computer system without the appropriate authorisation. Therefore, even if a hacker tries to get into a system but is unsuccessful they can be prosecuted using this law.

Although intention to do wilful damage cannot be easily proved, the act makes it an offence for a hacker to access and use a system using another person's user name, including e-mail, chat and other services.

The act also covers unauthorised access to different parts of a computer system, therefore, a person may be allowed to access one part of a system but not others, and the accessing of the other parts will be an offence.

<u>The penalties of breaking this act range from fines to imprisonment.</u>

Common Law Duty of Confidence

Common Law is also referred to as 'judge-made' or case law.

The general position is that if information is given in circumstances where it is expected that a duty of confidence applies, that information cannot normally be disclosed without the information provider's consent.

In practice, this means that all patient/client information, whether held on paper, computer, visually or audio recorded, or held in the memory of the professional, must not normally be disclosed without the consent of the patient/client.

It is irrelevant for example how old the patient/client is, or what the state of his/her mental health is; the duty still applies.

Three circumstances making disclosure of confidential information lawful are:

- where the individual to whom the information relates has consented
- where disclosure is necessary to safeguard the individual, or others, or is in the public interest
- where there is a legal duty to do so, for example a court order

How to protect information

To ensure confidentiality is maintained we must protect the information with which we are entrusted. This involves having the correct security measures in place to protect against loss, damage, theft or inappropriate destruction.

Security measures can be divided into three groups and the table below provides some examples:-

Physical Measures	People Measures	Electronic Measures
Ensure safe haven procedures Lock cabinets and doors	Character references	Ensure you have an effective passwords Don't share passwords
Do not swipe others into secure areas without escorting them	DBS checks	Report all Incidents
Do not discuss confidential matters in public	Identity checks	Encryption and secure emails
Do not share your Swipe card	Ensure your IG training is up to date	IT network security
Press ctrl alt delete to lock your computer	Follow Trust Policies and Procedures	Electronic audit trails
Confidential Waste	Telephones/mobiles/bleeps	Screensavers

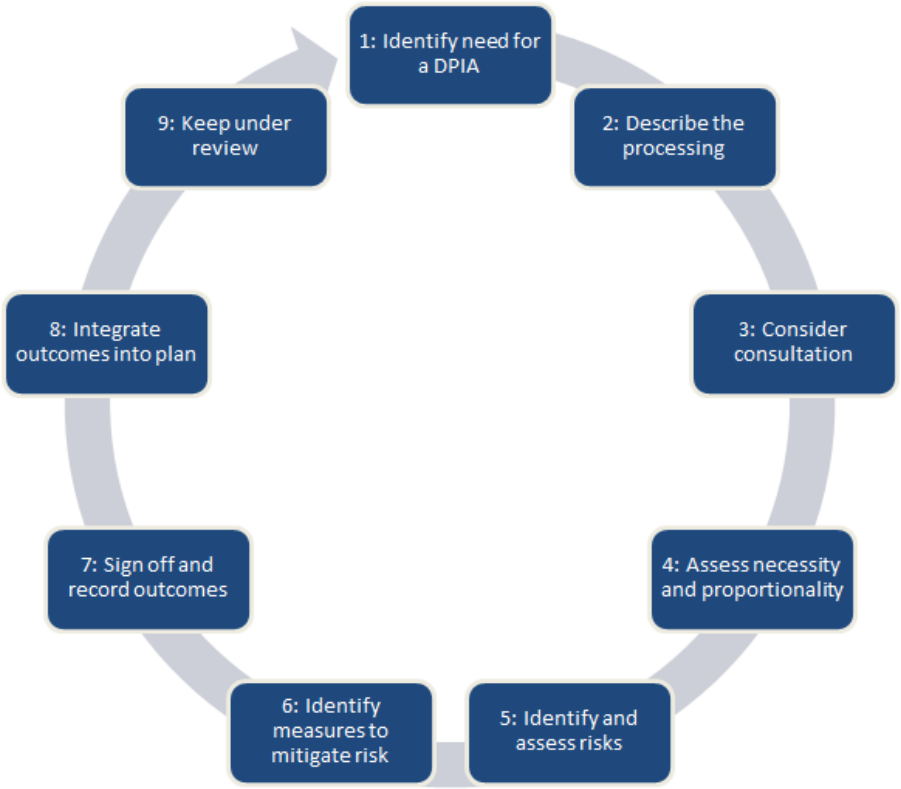
The key principle is to overlap security measures, whenever possible, to avoid situations where only one measure protects against the danger. Overlapping is good practice as it avoids total reliance on a single measure that may fail. For example, an outside door (physical measure) may be left open by staff, but security staff carry out routine checks (people measure) at the end of the day discover the open door and secure it hopefully before anything is stolen.

Data protection impact assessment (DPIA)

Data protection impact assessments (DPIA's) are used by MKUHFT to identify the risks associated with data protection obligations.

Data protection impact assessments are a mandatory requirement of the Information Governance Standard. They are designed to ensure that security and confidentiality of personal identifiable data is maintained during any new system, process or change in process to ensure risks are identified prior to implementation.

You must do a DPIA before you begin any type of processing which is "likely to result in a high risk". This means that although the actual level of risk has not been assessed yet, you need to screen for factors which point to the potential for a widespread or serious impact on individuals.



Even if there is no specific indication of likely high risk, it is good practice to do a DPIA for any major new project involving the use of personal data.

Caldicott Principle Guidelines

The key message from the Caldicott Report is that staff should justify every use of confidential information and routinely test it against seven principles

NEVER disclose confidential information if you are unsure about your response to any of these seven questions:

1 ***Do you have a justified purpose for using this confidential information?***
The purpose for using confidential information should be justified. This means making sure there is a valid reason for using it to carry out that particular purpose.

2 ***Are you using it because it is absolutely necessary to do so?***
The use of confidential information must be absolutely necessary to carry out the stated purpose.

3 ***Are you using the minimum information required?***
If it is necessary to use confidential information, it should only include the minimum that's needed to carry out the purpose.

4 ***Are you allowing access to this information on a strict need to know basis only?***
Before confidential information is accessed, a quick assessment should be made to determine whether it is actually needed for the stated purpose. If the intention is to share the information, it should only be shared on a need to know basis.

5 ***Do you understand your responsibility and duty to the subject with regards to keeping their information secure and confidential?***
Everyone should understand their responsibility for protecting information, which generally requires that training and awareness sessions are put in place. If the intention is to share the information, those people must also be made aware of their own responsibility for protecting information and they must be informed of the restrictions on further sharing

6 ***Do you understand the law and are you complying with the law before using/sharing the confidential information?***
There are a range of legal obligation to consider when using confidential information. They key ones that must be complied with by law are provided by the common law duty of confidentiality and under the Data Protection Act 1998.

7 ***The duty share information can be as important as the duty to protect patient confidentiality***
Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

If you have a question around the disclosure of medical or other confidential personal information you should seek advice from your line manager or contact the Information Governance Team. For serious and complex issues the Information Governance Manager will liaise with the Caldicott Guardian for advice and guidance.

Good Record Keeping

Commitment 8 of the NHS Care Record Guarantee
This promises that the NHS will take appropriate steps to ensure personal information is accurate. To meet this commitment you need to ensure that you have good record keeping and ensure records are:

Accurate

Make sure that when you create a file or update a record the information you are recording is correct and legible. Ensure that any factual mistakes are corrected or where appropriate reported to your line.

Up to date

Ask patients to confirm their details when attending appointments and ensure changes of address, name, next of kin details etc are updated as soon as possible.

Complete, including the NHS number

Incomplete or inaccurate healthcare information can put patients at risk. For example, the lack of certain information could cause a patient to be given the wrong treatment or advice.

Ensure patient records include their NHS number as this helps ensure the correct record is accessed for the correct patient.

Quick and easy to locate

You must ensure that records and their information can be quickly located, for example by using a logical filing system that allows easy retrieval of records.

Make sure you comply with any procedures that aim for consistent and standardised filing of records and for safe and secure records storage areas. If there are no such procedures, speak to your Line Manager, and the Records Manager or IG Manager if necessary.

Free from duplication

Good record keeping should prevent record duplication. Make sure one doesn't already exist before creating a new record. Having more than one record for the same patient can increase risks due to incomplete information.

Written contemporaneously

Good record keeping requires information to be inputted at the time of the event or as soon after as possible. Information is still fresh in your mind and will be available to others in ongoing patient's healthcare.

Record retention

When a record is no longer of immediate use, it can be closed. Closed records should be kept in with the Record Management NHS Code of Practice

Data Quality

Decisions based upon poor information may pose a clinical risk and potentially impact adversely on the quality of care a patient receives.
Poor quality information can also affect how we as a Trust get paid for the activity we undertake which can ultimately affect the services the Trust provides.
The Trust has an Electronic Master Index of patient information known as eCARE. All staff entering information onto eCARE are responsible for ensuring the information they enter satisfies the following criteria.

Accurate, i.e. a correct reflection of the patient journey	Valid, i.e. correct values for data fields such as NHS number
Consistent, i.e. national values used for recording information	Complete, i.e. all relevant data items populated (e.g. ethnicity)
Timely, i.e. information available at the time it is needed	

The Data Quality Team is responsible for monitoring the quality of the information entered onto eCARE. You can help by doing the following:

Reporting instances of duplicate patient records	Reporting Issues relating to how to record patient activity
Ensuring you take care when adding patient information to eCARE	Reporting any issues relating to patient information on eCARE

You can contact Data Quality on ext 86246 or alternatively by e-mail to:
data.quality@mkhospital.nhs.uk

Reporting incidents

Probably the worst position for any organisations is not knowing that a risk exists or that security measures are not working or are not being reported.
You are the expert in your work areas at assessing potential problems such as doors or windows that don't lock properly or confidential information left in public access areas. Early intervention helps minimise any impact and ensure corrective action can be swiftly taken so they do not reoccur for a second or third time.
We all have an obligation to act responsibly and to be aware of our local policies and procedures for reporting incidents. All new incidents should now be reported on Datix.

Anonymised Data

Anonymised data means the individual cannot be identified and therefore is neither personal nor confidential and does not need protection for the purposes of maintaining confidentiality. This data cannot be retrieved once it has been anonymised.

Psudonymised Data

Psuedonymised data is data that has been replaced by an artificially-created identifier (or code) so as to conceal the identity of the patient. This data can be retrieved.

Top information security tips

Secure Passwords
Ensure you use strong passwords, at least fourteen characters long that contain a combination of letters (both upper and lower case), numbers and symbols.

- Never disclose/share your password to anyone
- Never write your password down
- Never let others see you enter your password
- Change your password regularly
- Keep your reminders in a secure place not making it obvious that they are linked to passwords

Smartcards

Your smartcard provides you with a level of access to the healthcare information that you need as part of your job. You have a duty to keep patient information secure and confidential. Once you have been given a Smartcard, you must:

- Ensure that you accept the terms and conditions of use
- Keep it safe and secure and never share your password
- Never allow anyone to use you Smartcard – checks on access will be made and failure to comply with the terms and conditions can lead to disciplinary action
- Never leave you Smartcard unattended
- Report lost Smartcards immediately to the IT Helpdesk or the IG Team

Use of Temporary access cards (TAC) is very limited and will only be given out in exceptional circumstances.

Lock your screen

If you need to leave your desk. Press ctrl, alt, delete and enter to lock your screen.

Encryption

All portable media is encrypted, such as laptops, memory sticks, CDs etc. Thousands of USB sticks are lost or stolen each year causing personal, sensitive and confidential data to be lost or, more worryingly, exposed. Our Trust policy allows **only** the use of Trust approved password protected sticks. Speak to the IT Helpdesk to obtain one.

Email And Internet Use

Email should be used with caution and care taken when pulling addresses through from address lists. Ensure only staff needing to know the content of the email are included and DO NOT “reply to all” if it is not necessary.

Staff should bear in mind that all information produced can be made publicly available under the Freedom of Information Act if it is requested. Staff should not consider information sent or received through the email system as their private information.

You must ensure you read and abide by the email section within the Information Governance Policy which can be found at:- Information Governance Policy

The Trust allows staff to use internet for limited personal use, however, please "use it don't abuse it". Regular monitoring is undertaken on staff usage and the Trust has the right to withdraw this privilege should it find staff abusing this system. Further information can be obtained via the Internet section of the Information Governance Policy (please follow link above).

External post

When sending confidential information by post

- Place in a robust envelope and seal appropriately
- Mark **`private and confidential'**
- Clearly address to a named individual and ensure correct address is used
- If sending large quantities or highly sensitive information, ensure the data is double wrapped and sent by recorded delivery, special delivery or courier. Copies of patient's notes should be sent by special delivery.

Ward handover sheets

These continue to be found in inappropriate locations across the Trust: In public access areas (corridors, Eaglestone Restaurant etc), in the grounds (car parks etc) and even on streets outside the Trust. These documents contain highly sensitive and confidential information regarding our patients and should be treated exactly the same as a health record.

THINK: do not remove ward handover sheets or medical records unless absolutely necessary and **NEVER** take them home.

Telephone security

- Confirm the identity of the caller before releasing any confidential information
- Put callers on hold while locating the member of staff required
- Never name or discuss patients over the phone when in public access areas such as corridors, restaurants, on trains etc
- Do not text patient information on colleagues
- Do not use your mobile phone to photograph patients unless in an emergency
- Only leave messages on answer phones if the recipient has consented to the release or if the clinical need outweighs their right to confidentiality.

Conversations

Do not discuss a patient's treatment where you can be overheard, especially in public areas such as corridors, lifts, coffee shops etc.

Destruction of data

When confidential, sensitive or person identifiable data Is no longer required, place it in the shredding bin (Blue Wheelie Bins).

NHS number

Trust staff should be using the NHS number (where applicable) in all communications regarding patients, as this is classed as the patients unique identifier.

Training

Ensure you and your colleagues undertake your annual IG mandatory training. Ignorance is not an excuse – you **must** be aware of the basic requirements and keep up to date with the latest information and guidance to ensure a confidential service.

Work with the IG Team to determine what additional measures you can take to protect the information held in your work area

Access to Health Records

Access to Health Records now falls under the remit of the Data Protection Act and gives people the right to apply to access their personal information and receive copies if required.

Who Can Have Access

Patient	Authorised person on behalf of the patient
Parents	Children (under the age of 16)
Patient Representative	Persons who may have a claim arising out of a patient's death
Solicitors	

Children also have rights to privacy and can be deemed responsible at the age of 12

Before issuing the record the following checks need to be undertaken:-

No Third party information held in the record	No misfiling
There is nothing in the record that could cause the recipient any harm or damage	Consultation with an appropriate healthcare professional may be considered necessary

All requests are **Free of charge** and must be dealt with by the Information Governance Department and must be responded to within 30 days under the law, however, NHS Best Practice stipulates that this should be achieved within 21 days.

If a patient is on a Ward or within an Outpatient Clinic and requests a copy of their results these can be provided following consent of the treating Clinician. Requests for full sets of records **MUST** be directed to the Information Governance Department. Patients have the right to view their records whilst on the Ward, further information can be found within the Information Governance Policy located on the intranet.

Information Security – social media

As previously stated the rules on confidentiality still apply even after you have left the workplace. The rules of confidentiality must also be followed when using social networking sites such as Facebook and Twitter.

- Do not accept patients as Facebook friends
- You must not release any information on a social networking website which you have obtained as part you your job role (for example `guess who I saw at the hospital today?'
- You must not discuss any aspect of patient care on a social networking site, even if you believe you are chatting to the actual patient
- Images taken on recording equipment (such as camera phones) must only be taken and used with the explicit (written) consent of the individual(s) in the image. Under no circumstances may these images be posted onto a social networking site.
- Be careful if taking pictures that no patient information is in the background
- Defamatory remarks about the Trust or any of its employees must not be made. What may be considered to be "letting off steam" about a work situation can potentially be read by someone who may take offence at the content of a posting
- The date and time that comments or photos are "posted" are often visible on these sites. Please bear this in mind if using them at inappropriate times (for example, during working hours)
- Social networking sites should not be used for raising and escalating concerns (commonly referred to as whistleblowing). For further guidance, see the Trust's policy for staff when expressing concerns about standards of care or other Trust activities.
- Be aware that even in your private life, what you post on social media may be subject to disciplinary action.

Freedom of Information Act 2000

The Act places a duty on organisations to supply information to individuals who make a written request and allows **any** individual anywhere in the world to request information from a public authority. However, this is restricted to **non-personal corporate data** such as patient activity statistics, ward refurbishment costs etc. It aims to make public sector bodies more transparent and accountable. It also helps people to better understand how public authorities carry out their duties, why they make the decisions they do and how they spend public money.

All FOI requests must be responded to within 20 working days of the Trust receiving the request. If you receive an FOI request directly, please forward it immediately to :

Foi.PublicationSchemeCo-ordinator@mkuh.nhs.uk.
Remember it does not have to state it is a request under the Act.