Information Governance Manual Training Booklet

Introduction

This booklet is aimed at staff that do not access a computer whilst working for the Trust. If you have access to a computer, then you must complete the IG refresher training available via your MAST training record.

Information Governance Training is mandatory and must be completed annually by all staff regardless of the role you undertake in the organisation.

Questions

Please feel free to contact the Information Governance (IG) Department:

- If you have any questions or queries about this booklet or any topic that has been covered
- For any other information and guidance about IG.

The IG Department can be contacted via the details below:

Email	**Phone**
fhft.information.governance@nhs.net	01753 80 6726
Address	
Information Governance Department, Larch House, Frimley Park Hospital	

Once you have read this booklet, you will need to complete a short multiple-choice assessment. Your assessment has been given to your Line Manager or you can contact the IG Department above to request a copy.

Please complete the assessment and return it to the IG Department for marking (see details above). Upon marking the assessment, if you have passed (achieved 80% or more), your training record will be updated to reflect your successful completion.

The purpose of this Information Governance Booklet is to:

- Provide a basic understanding of information governance
- Make you aware of the Trust IG policies and procedures; and
- Make you aware of any IG incidents that have happened so staff can learn from them.

Key Contacts

The Trust has several layers to the organisational structure for Information Governance, some of the roles listed will be referred to during this training:

Senior Information Risk Owner (SIRO)

The Senior Information Risk Owner (SIRO) must be a Director-level member of staff or member of the Senior Management Team. They have overall responsibility for the organisation's information risk. The SIRO also leads and implements risk assessment process for information and cyber security risk across the organisation.

The Trust's SIRO is Nigel Foster – Director of Finance and IM&T

Caldicott Guardian

The Caldicott Guardian is a senior person in the Trust who has overall responsibility for protecting the confidentiality of patient and service-user information. They also are responsible for enabling appropriate information sharing and acting as the 'conscience' of the organisation.

The Trust's Caldicott Guardian is Timothy Ho – Medical Director.

Data Protection Officer (DPO)

Under the Data Protection Act, the Trust are mandated to appoint a Data Protection Officer who specialises in Data Protection law. They have overall responsibility for informing and advising the organisation about complying with the legislation, monitoring compliance and acting as a point of contact for the regulatory body.

The Trust's DPO is Nicola Gould – Head of Information Governance

Information Governance (IG) Team

All the above roles are supported by the Information Governance (IG) Team who in addition are also responsible for ensuring that the IG programme is implemented throughout the Trust, including expert knowledge of the relevant legislations and how to comply with them and for the completion and annual submission of the Trust's Data Security and Protection Toolkit (DSPT)

Introduction

The Information Governance Team at Frimley Health work with departments across the organisation to support and enhance work undertaken with regards to:

- Security of information
- New systems or processes being implemented
- Processing and handling of Personal Identifiable Data (PID)

We aim to provide you with knowledge, guidance and answer and questions that you may have and are responsible for formulating Trust policies and procedures to keep information secure such as:

- Email Policy
- Destruction of confidential waste
- Accessing information
- Incident reporting

All our policies and guidance documentation are available on the Trust's intranet known as 'Ourplace'. If you require access to any documentation, then ask your Line Manager or contact us directly.

What is Confidential Information?

Information provided to the Trust by patients and members of staff about themselves and/or their health is **confidential.**

This information is confidential, as it has been given with the expectation it will be kept secret, secure and not shared with staff who are not involved with their care.

Any patient information is confidential e.g:

- Name / date of birth
- address / telephone number
- Appointment date/time
- Reason for treatment,

Staff members who are being treated within the Trust also have a right to expect the same level of confidentiality.

Confidential information cannot be used or shared with anyone who is not involved with the care of the patient.

What confidential information do I have access to?

The different ways you might have access to confidential patient information whilst working in the Trust are:

- using a patient's name to transport them from one ward to another
- using a patient's name to process their meal request
- talking to a patient or seeing a patient whilst they are in the Trust
- entering a ward to repair some medical equipment
- transporting medical records or handling Trust post
- removing confidential waste bags from around the Trust
- cleaning an office or ward
- serving patients in the café or restaurant
- answering a phone call from a patient
- seeing a friend's medical record when working in the Trust

All staff have a responsibility to keep information safe and secure within the NHS regardless of the role that you undertake.

Any patient information which you see, hear or use must be kept confidential and only shared to support the care of the patient, even if this is someone you know.

Seeing a person or their medical records whilst working in the Trust is confidential information and cannot be discussed with the person, unless they choose to approach you or discuss the reason they are in hospital. To discuss with another person who you have seen in the hospital is a breach of confidentiality, even another member of staff.

Data Protection Act (DPA) Legislation 2018

The DPA Legislation relates to information about living identifiable individuals.

You are automatically covered by this piece of legislation until the day you die.

Whilst it is known as the Data Protection Act 2018, you may also have heard it referred to as the General Data Protection Regulation (GDPR) which came into force on the 25th May 2018. When the UK leaves the European Union, GDPR will no longer be applicable leaving the Data Protection Act in its place.

Anytime the Trust plans to use personal identifiable data in a different way, a Data Protection Impact Assessment (DPIA) must be undertaken to ensure that the rights and privacy of an individual's information are not impacted.

Individuals have increased rights under the legislation. Some of these are:

Right to be informed on how the Trust uses their information

Leaflets entitled 'Your Information' for patients and staff are available and a further detailed version is available on the Trust's online Privacy Notice:
https://www.fhft.nhs.uk/your-visit/privacy-policy-how-we-use-your-information/

Right to obtain a copy of information held about them

Medical records of a patient are the Trust's property and must be kept secure. If the patient is currently in the Trust being treated, they can request to review their current episode of care records with the relevant clinical staff.

Copies of records can be requested via the Access to Health Records Team. These are requested via an electronic form. If you wish to request a copy of your staff record, this can be done so via the Human Resources Department.

Right to processing and amending data

An individual has the right to request that the Trust:

- Stops or restricts the use of their information / information erased
- Rectifies errors identified within information that is held by us

All requests must in writing and sent to the IG Team via fhft.information.governance@nhs.net. Requests will be reviewed and responded to within 1 calendar month.

Data Quality

Every member of staff has a legal responsibility to check with patients that their information is accurate and up to date e.g. when transporting a patient down to x-ray checking that their name and date of birth is correct, if a patient identifies to you that their details are not correct these should be reported to the Nurse in charge immediately.

The Information Commissioners Office (ICO) is the UK's independent regulator set up to ensure organisations comply with the Data Protection Act and keep an individual's information secure and private. The ICO can fine an organisation up to £17 million (20 million Euros) where they have failed to meet the requirements of the new law.

As of April 2019, the total number of fines issued to health care related providers is over £1.9million.

The ICO will investigate complaints made by the public/patients about how an organisation has handled their information as well as providing guidance for organisations themselves.

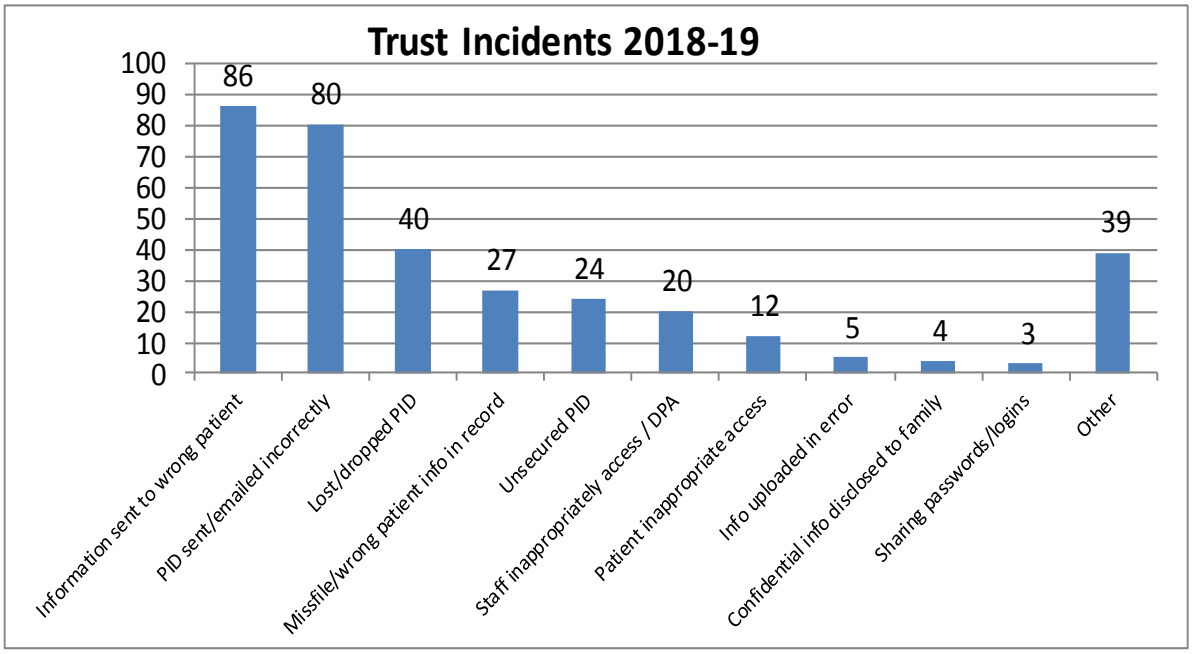
It is also worth noting that whilst the organisation can be fined, individual staff who have committed a criminal offence under the Act, such as accessing patient information without the consent of the patient or the Trust, could receive a criminal conviction and an unlimited fine.

There have been 5 documented criminal prosecutions against NHS staff **in the last year** by the ICO, against individuals who have inappropriately accessed patient records when they were not involved in the care of the patient.

The most common IG Incidents … and how to avoid them!

It is hard for an organisation and its staff to comply with the above laws all the time, as individuals make mistakes and accidents happen. It is the way that we learn from our mistakes or mistakes made by others which make the difference.

The mistakes highlighted in this section are the most common ones that have occurred in the Trust in 2018-19, a brief overview is documented in the graph below:



What does this mean for me?

All staff must ensure any patient or staff information is always protected and kept secure, for example:

- Always locking doors/cabinets when leaving an office unattended.
- Challenging individuals if they are not wearing a hospital ID badge and you do not recognise who they are when they are trying to access restricted areas of the Trust.
- Ensure patient information is not left unattended:
  - confidential waste bags are not left in a public / open corridor;
  - post bags are not left outside an office in a public / open corridor;
  - placing any piece of paper which has patient information on it into a confidential waste bag (blue or white bag).
- Not talking to your friends or neighbours about the patients you have seen or have spoken to in the hospital, or conversations you have overheard.
- Ensuring patient information is always in an envelope or secure medical records bags when being transported.
- Not disclosing any patient information over the telephone unless you have confirmed the identity of the caller and know they have a right to access the patient information.
- Knowing what an incident is and how to report it.

The Data Protection principles state that data must be kept accurate, secure and must be relevant. All employees are responsible for their own actions and need to comply with the Trust's policies and procedures – failure to do so could lead to disciplinary measures and possible legal action.

Trust procedures

Confidential Waste

Any piece of paper which has staff or patient information written/typed on it, e.g., name, address, date of birth, hospital number is confidential information and must be placed in one of the Trust's blue or white confidential waste bags.

These **must** be kept secure whilst waiting for collection in a locked office and away from public areas.

Recycling waste

All paper placed in recycling bags cannot contain any information relating to a member of staff or a patient. Any information which contains this type of information must be placed in a blue or white confidential waste bag, which as detailed above **must** be kept secure whilst waiting for collection in a locked office and away from public areas.

Hearing Confidential Conversations

When you overhear members of staff discussing the care of a patient, you must move away to provide privacy.

If you overhear a conversation between a patient and their relative, you must move away to provide them with privacy, and do not discuss the conversation with anyone. Staff must hold conversations about a patient in a secure/private area e.g. meeting room, Ward Manager's office and not in a public corridor.

Loss of Patient information

The Trust has had multiple incidents reported where staff have dropped documents in public places. This has included sheets found in corridors, the Trust car park, buses, bus stops and even the local High Street!

If you identify that patient information has been dropped or left around the hospital or externally, please pick it up give it to your Line Manager and log it as an incident.

Transfer of a patient's clinical records inside the hospital

Where these are transported with the patient, they must be handed to the member of staff and not the patient, there have been many incidents were patients have been found reading their clinical records unsupervised as they were handed their clinical records to hold whilst being moved around the hospital, this is against Trust policy.

Transporting clinical records
When transporting medical records these must not be left unattended in a public corridor, e.g., trolleys of medical records must always be accompanied.

Numerous incidents have occurred, when staff have left the clinical records in the back of a wheelchair after transporting the patient around the hospital. Always remember to pass the clinical records to a member of staff when moving a patient. If you find a set of clinical records left in the back of a wheelchair, you must remove them and hand them to your Line Manager to log as an incident.

Seeing a patient
If you see a neighbour or friend in the hospital, you must pretend you have not seen them, unless they approach you.

The fact they are in the hospital being provided treatment is confidential. If they want you to know why they are in the hospital, they will let you know.

Additionally, when you go home, you must not discuss with friends and family the patients you have seen in the Trust.

However, if you are asked general information about the Trust, i.e., what the visiting times of the hospital are, you can disclose this, as the information is not confidential or sensitive.

Security of offices
All offices and department should be locked when left unattended to ensure any confidential information contained in them is always secure.

Reporting Incidents

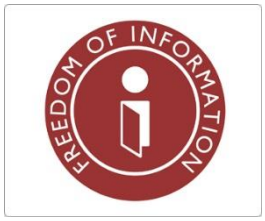
An important part of keeping information secure is to learn from past mistakes. This is achieved when staff report incidents and/or weaknesses in the Trust's security.

All staff must report any problems they see, for example:

- if doors or windows are not locking properly
- when staff place confidential information into normal waste bins
- when staff leave confidential waste bags in public corridors
- staff are not locking offices when left unattended
- when patient information has been dropped on the floor, found in a wheelchair or left in a public place, e.g., toilets, canteen
- staff have left patient information on printers or photocopiers
- Where patient information has fallen out of a record and is found on the floor, car park or outside the Trust.

All the above has and does continue to happen; therefore, it is crucial that all staff are vigilant and actively report concerns or incidents to your Line Manager as soon as they happen.

Freedom of Information Act 2000



This law gives anyone the right to request information from the Trust.

What must the Trust do?

The Trust must tell the person requesting information whether or not the information is held and provide a copy of the information requested within **20 working days**.

Does the Trust have to provide all information requested?

No, there are some reasons why the Trust does not have to provide the information which has been requested. When this is the case, the Trust must tell the person the reason for not providing the information.

What does this mean for me?

As a member of staff, any person could ask you for some information about the Trust. If a person asks you for information, please direct them to the FOI Team who can be contacted on fhft.foi@nhs.net.

Some examples of FOI requests

- How much money is spent on food for patient meals, repairing hospital equipment, purchasing equipment for patients, on cleaning the hospital, on Trust car parking?
- How many staff work in the transport, catering, estates, housekeeping departments?
- How many reported thefts have there been in the past year?
- How many times has the Trust called in pest control experts?
- What is the Trust's process for destroying IT Equipment?
- What are the visiting times of the hospital wards?
- What is the number of complaints from patients relating to sightings of any ghosts?

Records Management

All information created by you whilst working needs to be kept for a set period of time. The Department of Health provides guidance to NHS Trust on how long to keep their records.
If you handle any information and are not sure where or how long to keep the information, please ask your Line Manager.

Cyber Security

Although your access to the Trust network is limited, please be aware that the biggest cause of IG incidents is through emails being sent to the wrong recipient or spam/fake emails being received.
Whether you are at work or at home, always be careful when sending emails. If you receive something that looks -suspicious, do not click on any of the links and exit the

page e.g. a website stating that you have won a cash prize and to click on the link and enter your bank account details.

Assessment

Now you have read this booklet, please complete your IG Training Assessment and return it to the Information Governance Department.