Frimley Health NHS
NHS Foundation Trust

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, you must complete the IG refresher training electronically. Information Governance training is mandatory and must be completed annually by all staff.

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 is split between the two main hospital sites, contact details for the Information Governance Department are:

Frimley Park site	**Heatherwood & Wexham Park site**
Telephone: 01276 52 6607	Telephone: 01753 63 3875
Email: information.governance@fhft.nhs.uk	

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 to request a copy.

Please complete the assessment and return it to the relevant site's IG Department for marking. 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.

Introduction

Information is vital to an organisation, without it an organisation would be unable to carry out its functions. When the information is about patients or service users, any issue that disrupts its availability or compromises its accuracy can impact on the ability to provide a health and care service. Therefore, we must all follow the right processes to protect patients and service users and their information. Information Governance can be defined as:

"a framework of processes for handling personal information in a confidential and secure manner"

The Information Governance (IG) Department is responsible for reviewing and interpreting the different pieces of legislation listed below and setting up a framework of IG policies and procedures for the Trust.

The IG polices and procedure are reviewed in response to an incident either internally in the Trust or externally at another organisation to learn lessons from these incidents. Therefore, the policies and procedures are constantly changing and this training incorporates these changes, to ensure staff are kept up to date.

All policies/procedures and guidance produced by the IG Department is available on the intranet under Information Governance, please contact your line manager if you wish to obtain any guidance from the intranet.

What is Confidential Information?

Information provided to the Trust by patients about themselves and their health is **confidential.**

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

Any patient information e.g. name, address, date of birth, telephone number, reason for treatment, appointment date, appointment time is **confidential information**. Staff members who are being treated by their colleagues also have a right to this confidentiality.

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

Personal details of staff members that you work with are also covered by confidentiality.

What confidential information do I have access to?

The many different ways you might have access to confidential patient information whilst working in the Trust, these 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, restaurant
- Answering a phone call from a patient
- Seeing a friend's medical record when working in the Trust

All NHS staff have a responsibility to keep information safe and secure within the NHS. 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.

The Trust's Caldicott Guardian (Dr Timothy Ho, Medical Director) is the Senior Manager in the Trust who is responsible for ensuring all staff understand what it means to keep patient information confidential.

He also makes decisions when the Trust is asked to share information with organisations who are not involved with the care of the patient, for example the Police.

The Data Protection Act 1998

The Data Protection Act 1998 governs how organisations may use personal information - how they hold, obtain, record, use and share this information.

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 has the ability to fine an organisation up to £500,000 where it has failed to comply with the Data Protection Act.

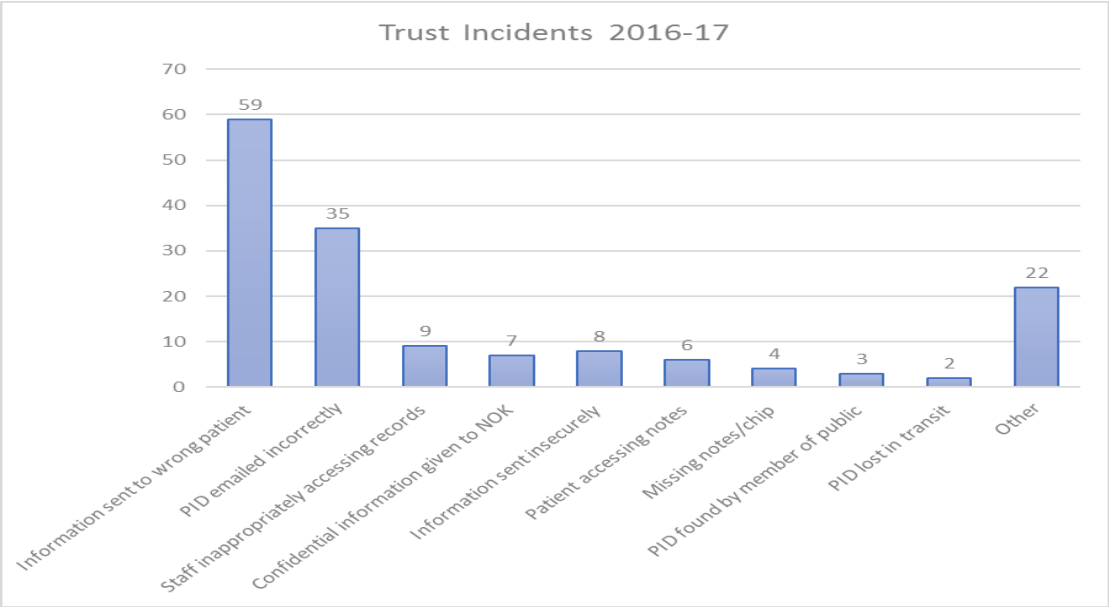
The ICO will investigate complaints made by the public/patients about how an organisation has handled their information as well as providing guidance for organisations themselves.

The Data Protection Act applies to both patient and staff information.

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 2016-17, see graph below, so this training booklet provides guidance to staff to help you from making the same mistake(s).



What does this mean for me?

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

- Always locking doors/cabinets when leaving an office unattended
- Challenging individuals you do not recognise who 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 each 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 patient information written/typed on it e.g. name, address, date of birth, 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 2 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 medical 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 medical records unsupervised as they were handed their medical records to hold whilst being moved around the hospital, this is against Trust policy.

Transporting medical 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 medical records in the back of a wheelchair after transporting the patient around the hospital. Always remember to pass the medical records to a member of staff when moving a patient. If you find a set of medical 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 are allowed to 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 secure at all times.

Reporting Incidents

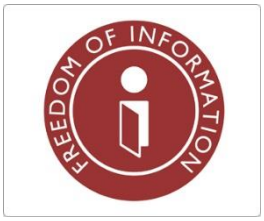
An important part of keeping information secure is to learn from past mistakes. This is achieved when staff report incidents and/or weaknesses in the Trust's security.

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 i.e. 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, outside the Trust

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

The Freedom of Information Act 2000



This law gives people 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 calendar 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 foi@fhft.nhs.uk

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?
- The Trust's process for destroying IT Equipment
- Visiting times of the hospital wards
- 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 dodgy, 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.

Once completed please hand to your Line Manager to send to the most relevant site office:

Frimley Park site	**Heatherwood and Wexham Park site**
Information Governance Department 2nd Floor Pine House Frimley Park Hospital	Information Governance Department 6th Floor Tower Block Wexham Park Hospital