Information Governance Refresher Training

All staff are required to undertake annual refresher training for Information Governance (IG) between 1st April and 31st March.

Previously, we have covered off in detail the different pieces of legislation that Information Governance covers, moving forward we look at how incidents affect the organisation, focusing on the requirement within the Data Security and Protection Toolkit (DSP) that we are mandated to complete to document the Trust's top 3 data security risks.

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 is 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 Data Protection Law, monitoring compliance, and acting as a point of contact for the regulatory body.

The Trust's DPO is Nicola Gould - Associate Director of IG

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)

Policies and Procedures
All Trust policies and procedures can be found on the Trust's intranet which is referred to as 'Ourplace'.

There is an Information Governance page set up which contains detailed guidance, policies and procedures to support staff in their day to day activities, ensuring that this meets our obligations under the relevant legislations. Further information can also be obtained from the IG Team directly.

You are advised to review Trust policies and procedures regularly to ensure you are aware of any changes which may have occurred. All major changes to policies will be communicated to staff, via the Trust global email/bulletins. Should you be found to be in breach of any Trust policy or procedure, you could be subject to disciplinary action. It is also possible that by your actions the Trust may incur significant financial penalties imposed by its regulatory body.

Legislation Recap

<table>
<tr><th colspan="2">Caldicott / Common Law Duty of Confidentiality
Relates to striking the right balance between protecting a patient's privacy and sharing of information to improve patient care.</th></tr>
<tr><td>The basic interpretation of the Common Law Duty of Confidentiality is:

Information cannot be disclosed outside the healthcare team without the patient's consent. All information that has been provided to the Trust by a patient has been provided in confidence.

There are some exceptions to this, information can be shared:
if there is explicit patient consent to share which is documented; or
where there is a greater public interest e.g. preventing serious crime (murder, GBH)</td><td>Personal Identifiable Data (PID) is information such as:
Patient's name, address, post code and date of birth
NHS number / Hospital number
Diagnosis or what treatment they are currently having in the hospital
Pictures, photographs, videos, audio tapes or other identifying images
Basically … anything that is likely to identify an individual!

Special categories of sensitive data
PID can also be considered as sensitive data if it falls into similar categories as below:
Ethnic Origin, Religious Beliefs, Political Orientation
Sexual Orientation, Genetic/Biometric, Health Care data</td></tr>
</table>

Data Protection Legislation 2018

Relates to information about living identifiable individuals

The General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA 2018) [1]became law in 2018

There are 6 principles that must be followed by organisations when processing personal identifiable data (PID), information must:

1. Be processed lawfully, fairly, and transparently
2. Be collected for specified, explicit and legitimate purposes
3. Be adequate, relevant, and limited to what is necessary
4. Be accurate and kept up to date
5. Not be kept for longer than necessary
6. Be kept secure to prevent unauthorised or unlawful processing, accidental loss, destruction, or damage to the data

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.

You must contact the IG Team if you are considering any of the below that involves using data:

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

Right to be informed on how the Trust uses their information

The Trust details how information is used 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:

[1] The UK left the European Union (EU) at the end of January 2020 and was in a transition period, once this concluded on the 1st of January 2021, the GDPR no longer became applicable leaving the Data Protection Act 2018 in its place.

• new service • change of service • purchase of a new system	• 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.

Other things to bear in mind about Data Protection

Data Quality	Information Sharing with External Organisations
Every member of staff has a legal responsibility to check with patients that their information is accurate and up to date e.g.: • Name / Date of birth • Address / Contact numbers • Next of kin • GP information The benefits of having the correct information are: • Patients can be contacted when needed by the Trust e.g. remind them about their appointment, booked for further treatment • Stops staff from creating duplicated records • Reduces staff administration time • Reduces complaints and reduces the potential for a breach of data or confidence • Helps to ensure that the Trust receives the correct funding for the treatment provided to patients It is a responsibility of all staff when meeting patients to check the accuracy of the information we hold to enable the Trust to	PID can be shared with consent of the individual. The Caldicott Principles must be followed, ensuring that the information being shared is: • Necessary / Proportionate • Relevant / Accurate • Timely • Secure **Golden Rules of Information Sharing** • Receive the request in writing • Confirm the reason the information is required • Confirm the identity of the person you are sharing with • Be fully satisfied that it is necessary to share • Obtain the patient's consent to share • Don't share more information than is necessary • Ensure that the information is shared securely • Record what information is shared in the patient's records. If the individual objects to any proposed information sharing, staff must respect their objection even if it undermines or prevents care provision.

ensure it is up to date. Staff must ensure that the data that the Trust holds on them is accurate and up to date. This can be done via the ESR Portal or by contacting HR directly.	However, in some instance's information could still be shared if there is an overriding public interest, e.g.: • Safeguarding children • Protecting other vulnerable people Staff should always check whether actual patient information is needed or if there is an alternative method e.g. removing the identifiable information completely or reducing it to one element.

Freedom of Information (FOI) Act 2000

Relates to information that is held by the organisation

Offers transparency across the public sector making organisations accountable to the public that they serve especially when it comes to finances and how decisions have been made.

Any member of the public can request information from us, for whatever purpose they wish, and we have a legal duty to:

- State whether the information they have asked for exists, and
- Provide a copy to them within 20 working days

A member of public might ask for information that you have either created or have been identified in e.g. meeting minutes, structure charts, or about you in your work capacity e.g. contact details, job description, salary banding.

What information can be requested?

Anything that is written down regardless of what format it is in can be requested by a member of the public. The typical types of information requested and released are:

- Policies and procedures
- Trust meeting minutes including Trust Board papers where major decisions have been made
- Copies of expenses for Board members
- Statistical information on the number of patients that the Trust has treated
- Financial spending information e.g. amount spent on agency nurses

What is the process to make a request?

The request must be in writing either via letter or by email. It does not have to specify that it is a Freedom of Information request, if in doubt forward to **the FOI Team as soon as possible.**

If you have received a request which you think maybe a Freedom of Information request, please forward it immediately to fhft.foi@nhs.net

The Trust has 20 working days in which to respond to a request from the date that it enters the Trust, please do not delay in sending the email to the address documented above. All requests are logged in the Information Governance Team and the final response is also sent from the department.

What information cannot be requested?

Whilst any information can be requested from the Trust, there may be times when we are unable to provide a requester with what they have asked for due to:

- The information is not held
- The information may already be in the public domain
- To release the information could potentially breach our legal Duty of Confidentiality to a patient or a member of staff
- The information that has been requested is commercially sensitive, have legal sensitivity or potentially could cause the Trust a security issue

	If any of the above applies, the Trust must justify why we believe that releasing the information could fall under an exemption. Unfortunately, it does not matter if the information requested is embarrassing or may hurt our reputation; there is not an exemption for this!

Consequences of breaching legislation

All organisations that process personal data are registered and monitored by the Information Commissioner's Office (ICO) who are the UK Regulatory Body. They can fine organisations up to a maximum of £17.3million[2] or 4% of their annual turnover depending on which is higher.

As well as this, if the organisation is identified as breaching an individual's rights, they can seek compensation where they have suffered damage or distress as a result of an organisation failing to comply with the Data Protection legislation.

As of March 2022, the total number of fines issued to health care related providers is over £1.9million. Some of the fines issued are documented below:

Date	Fine details
Dec-19	£275,000 – Doorstep Dispensaree Ltd For failing to ensure the security of its customers data by leaving approximately 500,000 documents in unlocked containers at the back of its premises.
Apr-19	£400,000 – Bounty (UK) Ltd For sharing personal data it held with 39 external organisations without their awareness
Sept-18	£175,000 – Bupa For failing to have security measures in place to protect data that became available on the dark web
Aug-18	£140,000 – Emma's Diary For selling on data to the Labour Party for targeted canvasing
May-18	£35,000 – Bayswater Medical Centre For leaving highly sensitive medical information in an empty building for 18 months
May-16	£180,000 – Chelsea and Westminster Hospital For an email breach relating to over 700 hundred individuals
May-16	£185,000 – Blackpool Teaching Hospital For publishing detailed personal data of its staff

The common themes surrounding the fines have been:

- Lack of staff training and awareness
- Lack of policies and procedures and/or lack of implementation
- Insufficient monitoring of policies and procedures
- Human error

The Information Governance Team routinely reviews IG policies and procedures following incidents that have happened within the Trust, or enforcement notices that have been issued to other organisations to learn from mistakes that have happened. As you will see further on in your training some of the mistakes that are made are sometimes the most basic ones but can have significant ramifications for organisations.

[2] Fines are in Euros – 10 million and 20 million Euros. They have been converted into pounds using current exchange rates, so will vary

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.

As of March 2022, there have been 5 documented criminal prosecutions against NHS staff by the ICO, against individuals who have inappropriately accessed patient records when they were not involved in the care of the patient. These are detailed below:

Date	Prosecution details
April-19	GP Practice Manager sent personal data to her personal email account without business need to do so.
Mar-19	Administrator accessed medical records without authorisation of 7 family members and 7 children known to them.
Nov-18	Administrator accessed electronic records of 228 patients and 3 staff members without consent.
Sept-18	Nurse accessed 5 patient records multiple times including blood results of a friend 44 times after they were discharged
April-18	Receptionist accessed the records of 12 patients without their consent.

It is a breach of Trust policy, the Data Protection Act, and the Common Law Duty of Confidentiality to access records of individuals (including patient and staff or even your own) when not involved in their care or without a legitimate work-related reason to do.

Even if the individual has given you permission to do so!

As mentioned above, a breach of the Data Protection Act is a criminal offence. This means that you as an individual can face a criminal prosecution, not just the Trust.

All main systems have audit trails which can be reviewed to monitor who has accessed an individual's record and this can be done upon a request from a Manager or if a complaint has been made. We also routinely conduct auditing of staff access across our systems to ensure that they are being used appropriately.

So now that we have recapped the different pieces of legislations, let's focus on data security and incidents.

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

Every member of staff has the responsibility to ensure that information is handled, stored, and transferred in a safe, secure, and appropriate way.

If you find anything that doesn't fit with this training or become aware of an incident happening, it is important that you report the incident on RL6 (the Trust's incident reporting system).

Please remember that by reporting an incident you are helping the Trust to learn, whether it is identifying gaps or weaknesses in the Trust's policies and procedures or something that has not gone well.

The majority of the reported incidents in the Trust are down to human error and staff making simple mistakes which result in a breach of Data Protection / Common Law Duty of Confidentiality.

The most basic incidents happen when people are distracted or rushing, one of the ways that this can be avoided is by utilising the 'Two Second Rule'.

Take 'two seconds' to ensure:

- The right letter is in the right envelope
- That information relating to another patient is not given out in error
- Correct email addresses are in the 'To' email field of sensitive information you are about to send
- Correct fax number has been selected
- That you have placed confidential information that is no longer required into the confidential waste bin at the end of your shift / end of the meeting
- That you have selected the correct patient on the clinical system
- That the notes that you are filing are in the correct folder
- That you selected the redacted spreadsheet instead of the patient identifying one to send out in an email
- That you have locked your computer before moving away
- That the PID that you have just used is locked away again when no longer required
- That you challenge anyone who is not wearing an ID Badge but claims to be a member of staff
- Only use Trust equipment for the storage of patient/staff information e.g., approved cameras, encrypted laptops and USB sticks, staff must not use their own cameras or phone to save and store any patient information

In a previous incident, where a member of staff did not follow the 'Two second' rule it resulted in breach of confidentiality. The repercussions of not doing so, led to 50 hours of work for the IG Team investigating, addressing, and resolving the incident with an actual cost of £1,500 to the Trust.

Any time an incident with personal data happens, it undermines patients/service users/staff member and public confidence in the Trust as to whether we can be **trusted** to keep information secure in the ways that we have stated above.

Further ramifications that we have experienced as part of processing complaints or incidents are that patients can lose faith in us. To the extent that they have cancelled appointments or been less willing to reveal important care information, affecting the care, advice, or treatment the patient receives. It has also broken working relationships with teams internally if they feel that their information has been accessed or shared inappropriately.

Some mistakes which involve either very sensitive patient information or caused an adverse effect are classified as a "Serious Untoward Incident (SUI)".

These incidents must be reported to both the Department of Health and the regulatory body – the Information Commissioner's Office (ICO). The Trust's investigation and management of these incidents is monitored by these external organisations.

Last year the Trust reported 2 Serious Incidents to the ICO, these were:

1. Staff member destroying paper records before they are scanned.
2. Staff members accessing patients record illegitimately.

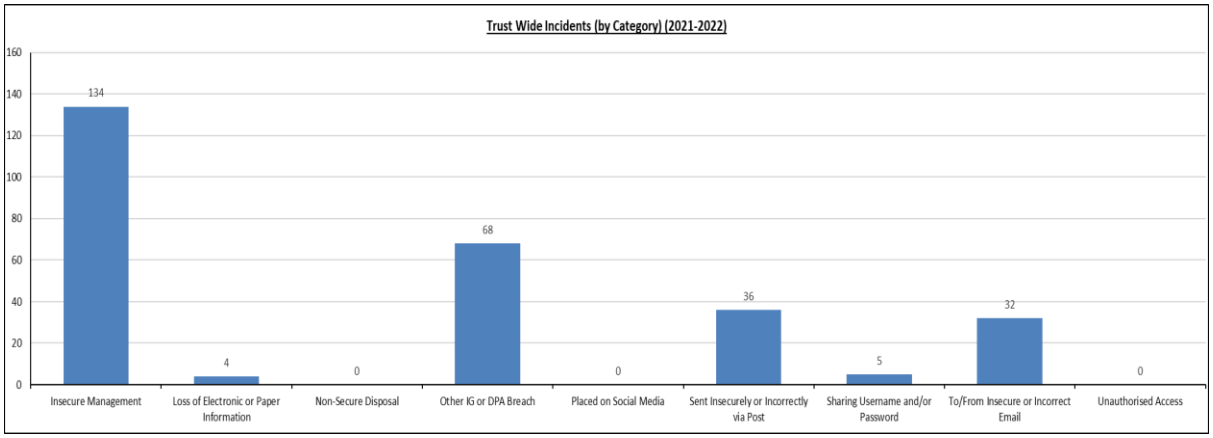
To date, no further action has been taken on any of them as the Trust had reviewed its processes.

Top three risks to data security to the Trust are:

1. Inappropriate access to information
2. Security of information in transit and at rest
3. Information being sent/given to the wrong person

The top three reported categories reported for 2021-22 were:

Types	**Examples are**
Insecure Management 134 incidents	Patient given another patient's information, Paperwork being left in wheelchairs or insecure areas, Information uploaded in error.
Information sent insecurely or incorrectly via post 36 incidents	Incorrect address on system, Included in another patient's letter, Address written on envelope incorrectly.
Information sent insecurely or incorrectly via email 32 incidents	Wrong email chosen from address book (both internal and global lists), Encryption function not used, Email address taken down incorrectly.



To help you understand how this links into incidents that we have had, we have provided an overview of the incidents and ways to avoid them are documented below:

Insecure Management

Information uploaded in error

There have been several incidents where identifiable information has been inappropriately uploaded to websites, messaging service apps and social media. Trust policy states that no patient or staff identifiable information should be uploaded to these types of sites without relevant approval.

Some incidents have been in error where pictures have unintentionally captured information in the background. The Trust does block access to social media and certain unsecure file sharing/blogging sites however if you require access for work purposes, a call should be logged on the IT Self Service portal.

Confidential information disclosure

We cannot assume that a patient is happy for information about their care and treatment to be shared with a relative or friend without their awareness. We must always check with the patient with whom they would like to have information about their care shared with, for example on their admission. This also applies to the patient's Next of Kin, as they do not have a legal right to be provided with detailed information about the patient's care.

Sharing information over the Phone

Detailed guidance on what information can be shared over the phone is available in the Guidance section on the Information Governance page.

To recap, if you receive a call requesting information about a patient who may or may not be in the hospital, only the most basic information must be given out providing you can ascertain the identity of the caller and the caller completes 3 security questions.

The 3 security questions should be initiated to confirm the identity of the caller and how they know the patient.

Examples of questions are:

- The patient's date of birth
- Their home address
- The name of their GP and which practice they are registered to
- Last time they came into hospital
- Next of kin information

The Trust policy is to **Confirm or Deny** if a patient is being treated at the Trust only, no clinical information can be shared unless you have the explicit consent of the patient to share the information this should be documented in the patient record.

If there is a requirement to leave a voicemail message, you must only leave a generic message e.g. 'it is xx from Frimley Health please call me back' and then provide the number.

When phoning other organisations, messages must not be left where there is not a voicemail introducing the service.

Lost / dropped PID
It was reported that there were incidents last year where staff dropped/left information containing PID in public places e.g. ward handover sheets / real time sheets / drug charts found in corridors, main corridor desks, Trust car park, buses, bus stops and even the local High Street!

If you find PID which has been dropped either around the hospitals or outside of the hospital grounds, please pick it up, give it to your Line Manager and log it as an incident. Please ensure that if you are carrying patient information, it is always kept with you and not left unattended.

Staff are not permitted to take patient information off site.

At the end of your shift, any paperwork containing patient information should be placed in a confidential waste bag if no longer required. Please do not take any patient information home e.g. handover sheets. To do so is a breach of Trust policy.

Wrong patient information in the record
The Trust has an obligation to ensure that the records it holds for its patients are relevant and accurate. If you are working with a patient's record, please remember to take the additional two seconds to ensure that you are filing/recording information into the correct record.

By not referring to the two second rule, it can take so much longer to resolve any misfile or information entered in error. It is always worth remembering that if a patient asks for a copy of their information under Data Protection and the record contains another person's information this is a confidentiality breach.

Confidential Waste
There are confidential waste bags (white or blue bags) available in all areas of the hospital for the secure disposal of identifiable or confidential information.

Anything that could identify an individual or is deemed as sensitive or confidential information must be disposed of in the confidential waste bags, this could be a name,

NHS number, staff assignment number, address, date of birth, hospital number.

Confidential waste bags must always be placed in a secure area or lockable cabinet when being used and when full and awaiting collection.

Unsecure PID
The Trust reported numerous incidents whereby patient, or staff information had been left insecurely either in an unlocked staff room, leaving a computer in a corridor open to patient information, leaving a lockable trolley or cupboard unlocked, leaving paperwork on your desk in an open plan office, leaving your smartcard in your computer.

It is **every** staff member's responsibility to ensure that any personal identifiable information that they use whether it be patient or staff information is always kept secure when in use and when no longer required.

Sharing usernames and passwords
All staff must lock their computer/tablet/phone when they leave it unattended. All mobile phones, laptops, computers, and tablets, whether work provided or not, should have a passcode set, the longer the passcode the more secure the device is.

There are two types of computer set up across the Trust, desktop clients and laptops and in clinical areas, iGels and Computers on Wheels (COWS).

For desktop clients and laptops, locking the computer will blank the screen and require you to enter your password in order to access it again. It is much quicker than logging off and logging on again and will protect the Trust network from inappropriate access by an unauthorised person.

In clinical areas, iGels and Computers on Wheels (COWS) are utilised to enable staff to use the virtual desktop environment for ease of use. The session can be accessed by tapping your ID badge to open the session and then tapping again to place the session on secure hold, allowing other staff to use the device under their own profile when no longer required by yourself. This removes the requirement for members of staff to repeatedly log on and off and enables a seamless continuation of access.
It is a breach of Trust Policy:

- to let another person use your username and password under any circumstances.
- for an individual to use another person's username and password.
- to use a computer which is currently logged on as someone else.

If you see a colleague's device open and unlocked, remind them to follow one of the above approaches to protect their device in the future.
If anyone in your department is unable to log onto a system, they must contact the IT Service Desk via the Self-Service Portal available on the desktop of your computer.

<u>Information sent insecurely or incorrectly via post</u>

The key themes surrounding each of these incidents were:

- Incorrect address details entered on systems for patients.
- Putting 2 different patient's letters into the same envelope and sending.
- Handwriting the incorrect address on the envelope, and not checking before sending.

To avoid repeats of similar incidents, key points to remember when sending by post are:

- Make sure you are only posting information that is relevant to the person/patient you are sending to.
- Always **double check** the full postal address of the recipient, ensure the address is correct and always mark the post private and confidential.
- Window envelopes should be used wherever possible to minimise the risk of sending to the wrong person.
- If you are expecting a response to a letter you are sending out, ensure your full contact details are provided e.g. your name, title, and department

Should you become aware that a patient has received information belonging to someone else, please ask them to return it to the Trust and log it as an incident via RL6.

Information sent insecurely or incorrectly via email

The key themes surrounding each of these incidents were:

- Sending information from nhs.net to a different email without using the secure functionality.
- Selecting an external person in NHS.net thinking they were a Frimley member of staff and emailing detailed clinical information.

Key points to remember when sending information via email are:

THINK What type of email am I sending?	**New email** – Think about what you are sending and to whom by following the guidance on method and data below. **Reply** – Pressing reply will only send an email back to the person that sent you the email. It will not copy any attachments enabling you to ensure any new information you send is appropriate and not excessive. **Reply all** – Pressing reply all will send an email to everyone in the last email. It will not copy any attachments enabling you to ensure any new information you send is appropriate and not excessive. Be very careful to make sure all recipients are entitled to see the information you are sending. **Forward** – Forwarding an email will allow you to send the previous email to new recipients and will include any attachments and the previous email trail.

	Make sure the person you are forwarding the information to is allowed to see it and that they have the correct account to receive it. Check what information is in the email trail – is it appropriate for the person you are sending the email to, to see the information in the email trail?
HOW What is secure?	PID can only be sent from nhs.net to nhs.net or the list of exceptions which is available on the Information Governance page. If PID needs to be sent to any other email address, then [secure] must be placed in the subject heading which will encrypt the email being sent.
WHERE Who am I sending it to?	Check all recipients when sending an email including anyone who has been copied into it (CC or BCC). This is especially important if you press 'reply all'. NHSmail will automatically start to identify emails of previous recipients; you must make sure the correct recipient has been selected. Check all recipients have the right to see the information you are sending e.g. staff employed by the CCG are not permitted to receive any patient information. Check all email addresses are either @nhs.net or [secure] must be used. If sending to more than one recipient, make sure that it is ok for everyone you are emailing to have each other's email addresses if unsure or emailing to more than one patient/person outside of the Trust use the blind carbon copy 'BCC' function.
DATA What data am I using / sharing?	If you do not need to use/share PID then don't, where possible, use pseudonymised / anonymised or 'redacted' data. If you need to use PID, you must only use the minimum data possible. Any more than this will be considered excessive and would be a breach of Data Protection / Caldicott principles. When you have prepared your email always check for PID; this can be included in the content of the email, attachments, images, and even the previous email trail, so it must all be checked before sending. If you are using anonymised data, also check to make sure this has been done correctly.

Inappropriate access to information

Last year there were 22 reported incidents were information was inappropriately accessed.

Inappropriate access to confidential information
The Trust reported incidents of staff accessing or inappropriately divulging patient's or staff's record when they were not involved with the care and treatment of the patient or had a Trust/work related reason to.

Your access to the Trust network and the Trust systems are for work related purposes only.

Where you are provided access to a Trust system, this is to provide health care to patients or to undertake Trust business.

Examples of the type of access that would be deemed as a breach is.

- Checking when your partner's hospital appointment is
- Looking to see if your neighbour is in the Trust
- Check to see if the results of the blood test you recently had have come back yet
- To identify a colleague/friend's home address so you can post them a Christmas card
- To look up a colleague/friend's salary for your own information
- To check whether your colleague has applied for an internal position within the Trust

Where a record has been inappropriately accessed, the member of staff may be subject to disciplinary action and if they are a registered or a regulated professional, they could be reported to the regulatory body.

The Trust takes these types of breaches very seriously and can follow the disciplinary process which has previously resulted in members of staff receiving warnings through to dismissals.

The patient or staff member could make a formal complaint, and take legal action against the Trust, which has a significant impact on the Trust and the member of staff.

Earlier in this training, we documented what the legal ramifications for the individual could be, but the important thing to remember is that is that you should treat the information that you handle with respect and care. Think how you would expect your information to be handled when you have given it to someone else, would you want people reviewing your record or sharing your information without your awareness?

Other IG guidance
Can patient's record their consultations?
There is no legal reason to prevent patient's wishing to record their consultation/treatment for their personal/private use as it is deemed as note taking. However, it should be undertaken in an open and transparent manner with staff affected, consulted with before the recording is made.

Further guidance on patients recording in the care setting can be found on the Information Governance page

Where can I have a confidential conversation?
Any conversation that is likely to be around patients or staff must not be conducted in open space eg corridors. Over the years, there have been incidents whereby staff

have been overheard discussing detailed patient care and other staff or members of public have been able to listen in.

Always consider your surroundings and whether you are in the most appropriate area for the discussion that you are having. Is there a more appropriate place eg a meeting room, ward managers office?

Do I need to track clinical (day forwards/inpatient) records?
It is mandatory across the Trust to ensure a patient's medical record is tracked **every time** it is moved.

For all staff who handle/move a patient's medical record they must ensure they are tracked electronically using the functionality on the Trust's Patient Administration Systems (iPM at Wexham and PAS/Patient Centre at Frimley).

Cyber Security

As people use computers more and more criminals are inventing new ways to illegally access computers and the information held on them. Criminals aim to steal patient information for several illegal reasons such as:

- create fake online profiles
- extort money from patients or service users
- sell the data for financial gain
- steal people's identity
- dupe patients into buying bogus cures
- find out more information about relatives

Therefore, there is a need for staff to understand how to keep computers secure. Below is guidance for staff on how to do this.

Emails

STOP, THINK and CHECK before opening an email as it could be a fake email (also known as a phishing email).

Criminals use fake (phishing) emails to scam thousands of people every week. They are just waiting for you to click their fake links to websites or attachments in order to steal your information e.g. login details, bank account details, passwords. So be cautious about opening an email from people you do not know.

Using fake emails is also an easy way for criminals to install software onto the computer you are using which can record your login details for the criminal to see, which could then be used to access your email or bank accounts fraudulently. Therefore, if you notice that your computer at work is running very slow, or freezing when it never used to, it could have a virus, so please contact the IT Service Desk.

What should I do if I get a suspicious email?

If you suspect an email of being suspicious please attach it to a new email and send it to: fhft.SuspiciousEmails@nhs.net

Users can also report suspicious e-mails direct to NHS Digital.

Instruction on how to report suspicious emails and further information can be located on the Phishing page of the Trusts IT Support website.

Passwords

Strong passwords can help stop cyberthieves from accessing company information. Simple passwords can make access easy. If a cybercriminal figures out your password it could give them access to the Trust's network. Creating unique passwords that are a minimum of 12 characters helps secure access. A good way to create a strong memorable password is to join 3 unrelated words together, make it obscure and have fun: picklehousepansy

Trust Phones/tablets/computers

Do not plug any non-Trust device into a Trust computer. Previously a member of staff brought a CD from home and placed it into a Trust computer, the CD contained a virus which then corrupted the Trust network for 72 hours, resulting in many clinical systems not being available for staff to use, which had a huge impact on patient care.

Staff should not plug any personal device into a Trust computer to charge it e.g. a mobile phone / an electronic cigarette as this can disrupt / impact the running of the computer.

Untrusted websites

When using the internet, you need to take care in case you enter a fake website, which has been made to look genuine. There have been past incidents where criminals have copied a bank website and then recorded the login details of customers as they used the fake website. If when using the internet, a link/message appears stating you have won a cash prize and enter your bank account details to receive the prize, it is a fake website.

Digital 'Do's' and 'Don'ts'

Do	Don't
Read the Trust's Information Security, Email and Internet policies and seek advice from your Line Manager if any aspect of the policy is unclear.	Don't use your own computer / tablet / phone for Trust work unless it has been approved by your Line Manager.
Report immediately any lost or stolen computer/table/phone to the Trust and/or the Police as soon as possible.	Don't use work-provided computers / tablet / phone for personal use unless it has been approved by your Line Manager.
Report security warnings from your internet security software to Trust IT. They might not be aware of all threats that occur	Don't engage with anyone claiming that they are from IT Support if they are unable to provide evidence that they work for the Trust

Keep regular backups of the data stored on computers/tablet/phone.	Don't connect your work computers / tablet / phone to unknown or untrusted networks, e.g. public Wi-Fi hotspots.
If your company sends out instructions for security updates, install them right away or as soon as convenient. This also applies to personal devices you use at work. Installing updates promptly helps defend against the latest cyberthreats	Don't leave work-provided computers / tablet / phone in a visible / public place or unattended in your car.
Store your computers/tablet/phone securely when not in use.	Don't install unauthorised software onto a work provided computer / laptop.

For further information an interactive Cyber Security training module can be found under the corporate section of the Frimley Online Learning Portal https://learning.fhft.nhs.uk/

Conclusion

You have now completed the learning material and should be ready to complete the assessment.

If you have any questions about the training material or assessment, please contact the Information Governance Department: