Introduction to Information Governance

Have you got an assessment?

- This is your mandatory training on Information Governance
- You need to complete an assessment during this presentation
- 11 questions to answer
- Must be handed in at the end for marking!
- Need to undertake yearly refresher training between 1st April and 31st March

Information Governance at Frimley Health

- We work with departments across the organisation to support and enhance patient care
- We are experts in the different legislations so you don't have to be!
- We are here to provide you with knowledge, guidance and answer any questions you may have
- We help the organisation to learn from mistakes through incident reporting
- We formulate Trust Policies that are designed to keep information secure such as email, destruction of confidential waste and accessing information

Information Governance Department
0300 614 5728 (Ext: 145728)
fhft.information.governance@nhs.net
Information available on the Information Governance intranet page

What does Information Governance cover?

Caldicott / Confidentiality

Common Law Duty of Confidentiality and consent processes

Overseen by the Trust’s Caldicott Guardian

Freedom of Information Act 2000

Relates to information held by the Trust e.g. minutes of meeting, audit reports, director expenses etc.

Data Protection Act / General Data Protection Regulation

6 Data Protection Act principles detailing how to hold, obtain, use, record and share personal information

What is a Caldicott Guardian?

Senior person in the Trust responsible for:

- Protecting the confidentiality of a patient and service-user information
- Enabling appropriate information-sharing
- Acting as the ‘conscience’ of the organisation

The Trust’s Caldicott Guardian is the Medical Director - Dr Tim Ho

Seven Caldicott principles to follow:

1. Justify the purpose of using confidential information
2. Only use it when absolutely necessary
3. Use the minimum required
4. Allow access on a strict need-to-know basis
5. Understand your responsibility
6. Understand and comply with the law
7. The duty to share can be as important as the duty to protect confidentiality

What is confidential information?

- Private information about an individual
- Given to you – someone who has a legal Duty of Confidence
- Expected to be used and kept in confidence

All staff are obliged to keep information secure because of:

- Signed Trust contract
- NHS Code of Conduct/Caldicott principles
- Legal obligation – Common Law Duty of Confidentiality
- Professional Code of Conduct – NMC/GMC

What is confidential information?

Which of the below is confidential information?		Confidential	Non confidential?
A	Patient’s medical records?	✓	
B	Seeing a patient that you know in the hospital?	✓	
C	Copy of a hospital policy?		✓
D	Patient’s hospital number?	✓	
E	Number of patients who attended the hospital last year?		✓
F	Patient’s name and address?	✓	

Freedom of Information Act 2000

- Anyone has the right to ask for copies of information held by the Trust

Data Protection Act	Freedom of Information Act
Can only ask for information about yourself	Can ask for any information which is not identifiable to an individual
1 calendar month to process	20 working days

- People have the right to be told whether the Trust holds the information and to be provided with a copy.
- All requests must be made in writing via email:

fhft.foi@nhs.net

- Trust makes information routinely available on the Trust website

Freedom of Information Act 2000

Which of the below is a valid Freedom of information request?		Valid	Not valid
A	Please send me a copy of my medical record		✓
B	How much did the Trust spend on agency nurses in the last three years?	✓	
C	Please send me a copy of your Hospital Admissions Policy	✓	
D	When is my next appointment?		✓
E	Number of complaints relating to haunted buildings within your Trust	✓	
F	Patient’s name and address?		✓

Data Protection Legislation

- Protects your rights as a unique living individual to privacy of your information

- Six key principles for an organisation to follow that information should be:
  1. Processed lawfully, fairly and in a transparent manner
  2. Processed specified, explicit and legitimate purposes
  3. Adequate, relevant and limited to what is necessary
  4. Accurate and kept up-to-date
  5. Not kept for longer than necessary
  6. Protected by appropriate security

- Organisations must appoint a recognised Data Protection Officer (DPO) – Nicola Gould – Head of Information Governance

Data Protection Legislation – Your rights

- To be informed on how organisations uses and shares your information and for what purpose
  - Information available on the Trust's Privacy Notice and via 'Your Information' leaflets
- Patients/staff have the right to obtain a copy of information held about them
  - Free of charge and within 1 calendar month
  - Processed by the Access to Health Team for patients / HR for staff requests
- Right to rectification
  - Right to request that an organisation stops or restricts the use of their information or have information about them erased
  - Rectification of errors identified within information that it held by an organisation
- Ability for individuals to claim compensation for damage and distress
- Penalties for getting it wrong or lack of compliance

Consequences if we get it wrong!

ico.
Information Commissioner's Office

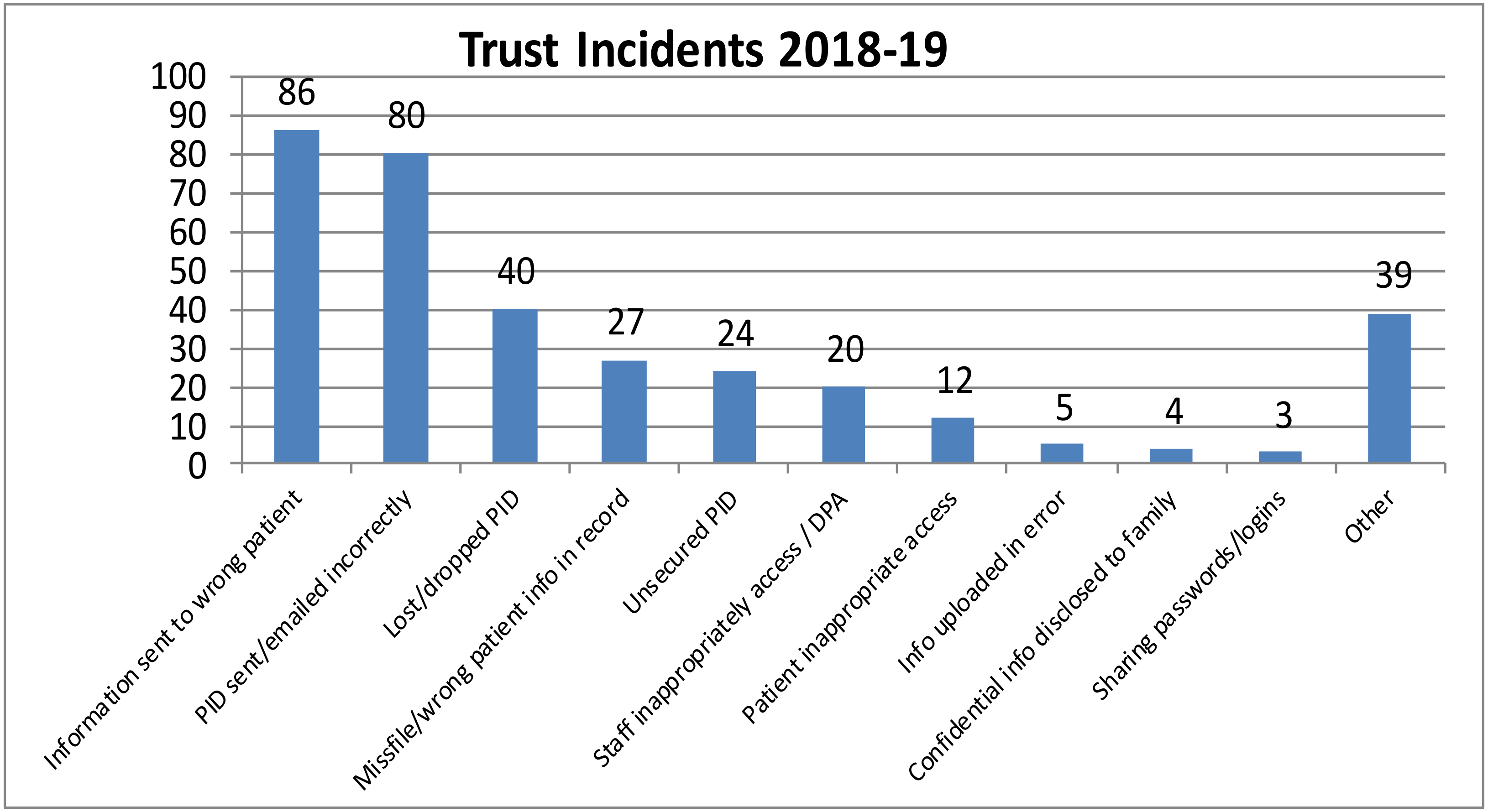
- All organisations that process personal data are regulated by the Information Commissioner's Office (ICO)
- Routinely produces guidance, codes of practice and can audit organisations
- Ability to impose fines of up to 20 million euros (roughly £17 million) or up to 4% of annual turnover
  - Jul-19 – British Airways - £183m for cyber security breach
  - Jul-19 – Marriott Hotel Chain - £99.2m for breach of their website
- To date the NHS has been fined over £1.9million, examples are:
  - Chelsea and Westminster Hospital fined £180,000 for email breach
  - Blackpool Teaching Hospital fined £185,000 for publishing detailed personal data of its staff
- Can prosecute organisations AND individuals
  - Apr-19 – GP sent personal data to her personal account without business need to
  - Mar-19 – NHS Admin accessed records of family members and children known to them

Learning from mistakes …

- Report on RL
- By logging an incident it helps the Trust learn from its mistakes
- The majority of incidents logged are down to human error
- Anytime there is an incident with patient information it undermines the confidence that people have in the Trust
- We investigate each incident/near miss to see where it has gone wrong and what learning there is to support and enhance patient care
- We review policies, procedures and guidance to identify where we can change and adapt if needed

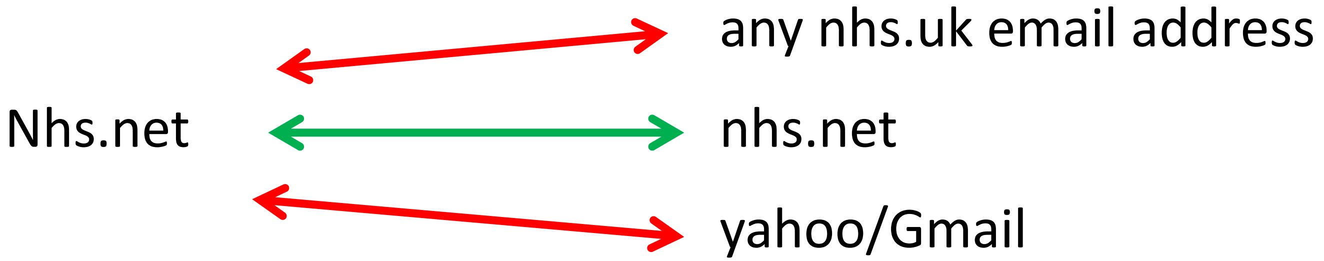
Finally … just because we have always had a process doesn't mean it shouldn't be reviewed and changed if needed!

Learning from mistakes …



Email Security

- When sending personal or sensitive data, only use secure accounts
- There are 2 ways of emailing securely:



- Or, when sending outside of nhs.net to nhs.net use [secure] in the subject heading

Things to remember:

- Check recipient list to ensure you are sending to the right person
- That there is a legitimate requirement to share the information and that you are doing so securely
- Check all attachments for any identifiable data
- If in doubt don’t send until verified

Network Security

- STOP, THINK and CHECK before opening an email.
- If you do suspect an email is not genuine, take these steps:
  - Do not reply / forward on or open attachments
  - Put the email in your junk or spam folder
  - Forward the email as an attachment to fhft.suspiciousemails@nhs.net
- If you have received an email containing patient information in error, delete it and log it via the Trust's incident reporting module

Untrusted websites

- If a web browser states that you are about to enter an untrusted site, be very careful - could be a phishing website that has been made to look genuine.

Information security

Log off or Lock devices

- Log off or lock your device as soon as you leave it. ALL mobile phones, laptops, computers and tablets, whether work provided or not, should have a passcode set.

Password Security

- The Trust has moved to single passphrases for all network accounts eg

’avengersassemble’ or ‘supercalifragilisticexpialidocious’

- For all other applications you should make passwords as complex as possible e.g. over 8 characters and use a combination of digits and symbols
- For complex passwords they need changing regularly

NEVER SHARE YOUR PASSWORD OR LET ANYONE ELSE USE YOUR LOGIN

Other ways to keep information secure

- **Physical records –**
  - Lock rooms, cabinets and lockable trollies.
  - File information away ensuring clear desk policy is maintained at all times.
  - Do not leave papers in public spaces including Nursing Stations or Reception Desks.
  - Put paperwork into a bag or folder to protect it. Do not transfer information unless you have to
- **Medical Records -** Ensure any Medical Records you are moving are tracked to their next location
- **Confidential waste –** Papers that contain personal or sensitive data must go in confidential waste. E.g. patient or staff identifiable data
- **Post –** Use sealed envelope, addressed correctly/use window envelopes, have Private and Confidential on the front, always check what you are sending is correct, if you can use secure email instead do
- **Fax –** Use secure machine and check number is correct, always use a Private and Confidential fax header

Confidentiality Scenario's

You answer the phone to a member of the public who is asking if their uncle is in hospital and what treatment they are having

What can you tell them?

3 security questions –

- Patient's name
- Date of birth
- Address/GP information

Confirm or deny they are there.
No further information to be given out over the phone

A member of the Police contacts you to ask for the names and addresses of patient's who attended the department in the last 24 hours

Should this be provided to them?

No

Request must be in writing with patient consent

If they are unable to obtain patient consent then request must be sent to IG Department

What would you do……..?

Your partner has been in hospital for some tests and asks you to check the computer system to see if their results are back.

Should you do this?

A member of staff is off sick and you want to send them a get well card so look at their ESR record to get their address.

Is this ok?

No!

You have been provided access to clinical and non clinical systems to provide health care to patients and conduct Trust business

If you are not involved in the health care of the patient or do not have a work related reason, you are not permitted to access their records or your own

The Trust has the ability to monitor and audit access and usage of network and systems