WHAT COUNTS AS AN INCIDENT – WHAT SHOULD I REPORT?

- Loss or theft of equipment (e.g. desktop PC) or removable media (e.g. laptop, CD, USB memory stick)
- Person identifiable data being sent insecurely by a member of staff (e.g. sending an unencrypted file via unsecured email)
- Breach of confidentiality/security of person identifiable data or sensitive information
- Finding any paper records about a patient/member of staff or business of the organisation, for example unattended on the printer or in the street.
- Patient or staff data being sent via internal/external post to the wrong person or not sent securely (e.g. a patient record not sent in a sealed envelope, marked confidential or addressed to an individual)
- Patient or staff records on view to the public (e.g. in an employee's car or on a reception desk)
- Discussing patient or staff personal information with someone else in an open area where the conversation can be overheard
- A fax being sent to the wrong person/fax machine (e.g. staff not following the Safe Haven Policy) or any fax received not in a secure area. If there is any doubt it is always best to report it.

I NEED MORE INFORMATION

There is information and forms to report incidents available in the Information Governance folder in the Corporate Business folder on the V drive

NHS
Brighton and Hove
Clinical Commissioning Group

THE STAFF GUIDE

Information Governance: reporting incidents and good practice

What is Information Governance?
Information governance brings together all the rules, guidance and laws relating to how we handle information to make sure we are protecting the details of patients and staff.

Why do I need to worry about it?

- To protect a person's right to confidentiality
- To make sure our organisation doesn't break the law – or get fined
- To make sure we are an organisation the public can trust

DOS AND DON'TS

Don't

- Don't share passwords or leave them lying around. Change them at regular intervals
- Don't use person-identifiable information unless absolutely necessary, anonymise the information where possible. Share only the minimum information necessary
- Don't share information without the consent of the person to which the information relates, unless there are statutory grounds.
- Don't gossip

DOS AND DON'TS

Do

- Protect all person-identifiable or confidential information that you come into contact with
- Shut/lock doors cabinets as required and keep paper records secure
- Keep all hard copy records containing person-identifiable or confidential information in recognised storage places that are locked when you are not there.
- Ensure mobile data devices i.e. data sticks, laptops etc are encrypted
- Log out of computer systems/applications when finished work. Lock screens/apply screensavers when PC is unattended.
- Make sure you cannot be overheard when discussing confidential matters. Be prepared to challenge colleagues if you see/hear this happening
- Report any actual or suspected breaches of confidentiality.
- Challenge and verify where necessary the identity of any person who is making a request for person-identifiable or confidential information and ensure they have a need to know. Phone back to check if necessary
- Transfer person-identifiable or confidential information securely
- Seek advice if you need or are asked to share patient/person-identifiable information without the person's consent and record the decision and any action taken
- Participate in induction, regular refresher training and awareness raising sessions on confidentiality

WHAT COUNTS AS AN INCIDENT – WHAT SHOULD I REPORT?

An information governance related incident relates to the breach, theft or loss of :

- information security
- personally sensitive/confidential information
- personally identifiable data (PID)

An **information security** incident is defined as any event that has resulted or could result in:

- Risk to the integrity of an information system or data
- Risk to the availability of an information system or information
- An adverse impact e.g. Damage to the reputation of a person or the CCG, threat to personal safety or privacy, legal obligation or penalty

Confidential material is any information disclosed from one person to another in circumstances where it is reasonable to expect that the information will be held in confidence.

Personally sensitive

Racial or ethnic origin

Physical or mental health condition

Sexual life

Committed offences

Any procedures for any offence committed or alleged

Includes sentencing decisions

Political opinion or persuasion

Religious belief or other beliefs

Trade union membership/ affiliation

Person Identifiable Data (PID)

Surname, forename and initials

Address, postcode or phone number

Date of Birth

Other dates (e.g. death or diagnosis)

Local Identifier (e.g. hospital or GP practice number)

Occupation

Sex

NHS Number

National Insurance Number