NHS

Hertfordshire, Bedfordshire and Luton
ICT Shared Services

Introduction to Information Governance

June 2017

CONTENTS

- What is Information Governance
- Confidentiality
- Data Protection
- Information Sharing
- Information Security

Information Governance

Information Governance is the controls, policies and procedures that need to be in place to ensure information is:

- Handled
- Obtained
- Processed
- Stored
- Shared
- Disposed of

Safely and securely

Information Governance

- Data Protection Act 1998
- Freedom of Information Act 2000
- Health and Social Care Act 2012 (section 251)
- Information Security Standards ISO/IEC-27002:27005
- Management NHS code of Practice
- The NHS Confidentiality Code of Practice
- Caldicott Principles
- The Records Management NHS Code of Practice
- Information Quality Assurance

Information Governance Toolkit

- Information Governance Assessment Tool
- Annual submission by 31st March
  - CQC, NHS England
- Organisations have to demonstrate compliance with the following:
  - Information Governance Management
  - Confidentiality and Data Protection
  - Information Security

Guidance for Care Homes Completing their first Information Governance (IG) Toolkit

Microsoft Word Document

Information Governance – Types of Information

PERSONAL INFORMATION:

This relates to Information about a person which would enable that person's identity to be established by one means or another. This could be fairly explicit such as an unusual surname or isolated postcode or items of different information which if taken together could allow the person to be identified. All information that relates to an attribute of an individual should be considered as potentially capable of identifying them to a greater or lesser extent .

SENSITIVE INFORMATION:

This can be broadly defined as that which if lost or compromised could affect individuals, organisations or the wider community. This is wider than, but includes, information defined as sensitive under the Data Protection Act 1998, e.g. an individual's bank account details are likely to be deemed 'sensitive', as are financial and security information about an organisation.

Information Governance – Types of Information

PSEUDONYMISED INFORMATION:

Pseudonymised data/information is anonymous to the people who hold or receive it (e.g. a research team), but contains information or codes that would allow others (e.g. those responsible for the individual's care) to identify an individual from it. (Also referred to as linked anonymised).

ANNONYMISED INFORMATION:

Anonymised data are data prepared from personal information, but from which the person cannot be identified by the recipient of the information.

Activity: What type of information do the statements relate to?

Characteristics		Personal	Confidential	Anonymised	Pseudonymised
A.	Is about a named individual's next hospital appointment				
B.	The information does not directly identify an individual				
C.	Might include names and addresses				
D.	No-one can link the information back to a specific individual				
E.	Identifying information will have been replaced with a code				
F.	The information directly identifies particular individuals				

iG INFORMATION GOVERNANCE

Data Protection Act 1998

- Processed Fairly & Lawfully
- Processing personal data for one or more specified & lawful purposes
- Adequate, relevant & not excessive
- Accurate & up to date
- Not kept any longer than necessary
- Processed in accordance with the “data subject’s” (the individual’s) rights
- Securely Kept
- Not transferred outside the EEA without adequate security in place

Caldicott Guardian

- Every NHS organisation should have a Caldicott Guardian to safeguard patient information and confidentiality

- It is usually someone with a clinical background

Caldicott Principles

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. Sharing information can be as important as the duty to protect patient confidentiality

iG INFORMATION GOVERNANCE

Freedom of Information Act 2000

The Freedom of Information Act 2000 provides public access to information held by public authorities:

- Public authorities are obliged to publish certain information about their activities
- Members of the public are entitled to request information from public authorities.
- Unless an exemption applies the organisation has to release the information. (if they hold it)
- The organisation has 20 working days in which to respond.

Information Sharing

In most cases you will need consent from the person before you can share information about them:

- Implied consent – when consent is implied by the behaviour of the individual
- Explicit consent – when full informed consent must be obtained, usually in writing

Information Sharing – Without Consent

Other reasons when we may share or disclose personal information:

- When the law requires e.g. court order
- To prevent harm to the patient or to others
- In the overriding public interest

Information Sharing

We Share because we care – Sharing Health records

https://www.youtube.com/watch?v=sD4QiquLZiw&t=90s

Information Security

It is the responsibility of all staff to ensure information is kept secure:

- How information is stored?
- How information is shared?
- How information is disposed of?

Aim is to protect the confidentiality, integrity and availability of information and systems

iG INFORMATION GOVERNANCE

Activity : Angelique (IT Technician)

Scenario

- Can I borrow your ID badge to get into the **Authorised Area***, I've left mine at home and I've only got this temporary pass!
- What would you do? Consider the options then look at the feedback on the next slide

*Think about the areas or rooms in your organisation that have restricted access

Options	
A.	Lend her the pass
B.	Tell her you cannot lend her your pass
C.	Escort her to the area and let her in

Information Incidents Data Loss/Breach

Danni’s Day

https://www.youtube.com/watch?v=gNZBLU_DPog

What Danni did wrong

PDF File

Information Incidents Data Breach

What is a Data Breach?

- Loss or theft of data or equipment on which data is stored
- Unlawful disclosure or misuse of confidential data
- Recording or sharing of inaccurate date
- Inappropriate sharing of information
- Equipment failure
- Unforeseen circumstances such as a fire or flood

What is a Cyber Breach?

A cyber related incident is anything that could (or has) compromised information assets with cyberspace.

- Denial of Service attacks
- Phishing emails
- Social Media Disclosures
- Web site defacement
- Malicious Internal damage
- Spoof website
- Cyber Bullying

Information Incidents Data Breach

Why do we report?

- Legislation requires us to report
- Transparency
- Allows controls to be put into place to minimise impact to the organisation
- Processes to be reviewed/updated to mitigate similar incidents occurring
- Avoid fines

Information Incidents Reporting

All staff have a responsibility to report IG incidents whether deliberate or accidental

- In the first instance your Line Manager
- The Incident Reporting tool within the IG Toolkit (level 2 and above)

https://www.igt.hscic.gov.uk/resources/HSCIC%20SIRI%20Reporting%20and%20Checklist%20Guidance.pdf

Information Incidents Reporting

Once a data/cyber breach has occurred, the following should be considered.

- Who should I notify in the first instance
- Who needs to be made aware of the breach
- Are there any legal or contractual requirements
- What documents need to be completed
- Does the breach need to be reported to the ICO (level 2)
- What lessons have been learned
- What needs to be put in place to mitigate further risk

How to report an incident

- Notify the nominated person who will lead investigation
- Notify relevant manager member by telephone or email
- Complete an IG incident form

Information Incidents Reporting

Completing the Incident Form

- Speed - report suspected breaches ASAP
  - We must report incidents to NHS Digital
- Details
  - What happened?
  - What should have happened?
  - When did it happen? Specify dates & times
  - Who is involved? Organisations, individuals, job titles, phone numbers, email addresses etc.
  - Have you done anything in response? Contact?
  - Quantify – type of information, is it PID, numbers of individuals affected

Anecdotal Evidence - Benefit of NHSmail in a particular Care Home

- Improved communication between providers
- Care Homes able to plan for residents ahead of time
- Savings to GP time
- Added value to residents' families
- Less use of Fax machines

Information Governance

Any Questions Please?

This training material has been produced by HBL ICT Services in association with Ruth Boughton, Information Governance Manager for Herts Valleys Clinical Commissioning Group