Client Information Transfer Sheet

Coventry Residential / Nursing Homes and Housing with Care working in partnership with Hospitals

Project Team

- Deanna Phillips - Adults Commissioning, Coventry City Council
- Carol Donovan – Information Governance, Coventry City Council
- Hannah Towle - REACT Coordinator, University Hospital Coventry & Warwickshire
- Kathryn Harris – Lead Nurse, University Hospital Coventry & Warwickshire
- Sue Kavanagh – Coventry PCT

The purpose of today's session

- To enable clear information regarding individuals to be exchanged between a care establishment and the hospital and vice versa.
- This will enable the hospital to quickly understand more about the individual so that care and/or treatment can be provided in a manner that takes into account that individual.

When to Use the Client Information Transfer Sheet

- A 'Client Information Transfer Sheet' is to be used in all circumstances when an individual living in a residential, nursing or 'Housing with Care' scheme is transferred to hospital and when individuals are transferred back to their care establishment.

Information Governance & Security

C Donovan
Information Governance Officer

Information Governance & Security

- Introductions
- Why do I need to know this?
  - Financial penalties
  - Prosecutions
- What type of information are we talking about?
- How could it go wrong?
- Examples of what you need to do to prevent it going wrong
- How do I learn more?

Information Governance & IT Security: Why Do I Need to Know This?

- **Legislation governs how we manage personal data**
  - Data Protection Act 1998
  - Human Rights Act
- **Information Commissioner investigates complaints and incidents**
  - Complaints from the public & other organisations
  - Self-reported incidents
  - Mandatory for the Health Service to report incidents
  - Financial penalty up to £500,000 per breach
- **Audits by the Information Commissioner's Office (ICO)**
- **Unlawful obtaining or accessing is a criminal offence:**
  - Up to £5,000 fine in a Magistrates Court
  - Unlimited fine in a Crown Court
  - Criminal record
- **CEO required to sign a public undertaking**

Information Governance & IT Security: Why Do I Need to Know This?

- **Increased Risk of:**
  - Financial penalties
  - Breach of confidentiality
  - Regulatory work being prejudiced
  - Additional costs from implementing remedial solutions
  - Human rights issues
  - Reputational damage and/or loss of confidence
  - Civil proceedings
  - Damage and distress claims leading to compensation payments
  - etc……
- **Employees**
  - Employment contract – Code of Conduct
  - Ensure you are aware of your responsibilities
  - Wilful breach may result in a criminal offence

Information Governance & Security: Financial Penalties – The Named & The Shamed

Midlothian Council	£140,000	Sensitive personal data of children & their carers sent to wrong recipients on 5 separate occasions
Powys County Council	£130,000	Details of child protection case sent to wrong recipient
Worcestershire County Council	£80,000	Emailed sensitive personal data about a large number of vulnerable people to 23 unintended recipients
North Somerset Council	£60,000	2 emails containing highly sensitive and confidential information sent to the wrong NHS employee
Hertfordshire County Council	£100,000	Faxing highly sensitive personal information to the wrong recipients – one fax was about a sexual abuse case (before the courts) the other about care proceedings
Croydon Council	£100,000	A bag containing papers relating to the care of a child sex abuse victim was stolen from a London pub
Norfolk County Council	£80,000	Disclosing information about allegations against a parent and the welfare of their child to the wrong recipient

Information Governance & Security: Prosecutions – 'Fingers in the Till'

Receptionist	2 year conditional discharge £614 costs	Unlawfully obtained her sister-in-law's medical records to find out what medication she was taking
Former gambling industry worker	3 year conditional discharge Order to pay £1760 to Cashcade Ltd £830 costs	Unlawfully obtained and sold personal data about 65,000 on-line Bingo players
Employee of personal injury claim company	£1,050 fine £1,160 prosecution costs £15 victims' surcharge	Obtained personal information of about 29 patients who had received treatment, following an accident, from a walk-in centre. Used the information for claims leads The information was supplied to him by his girlfriend who worked there
Bank cashier	Fined £800 £400 costs £15 victim's fee	Used her position to access illegally personal details of a sex attack victim

Information Governance & Security: What Types of Information Are We Talking About?

- **Personal & Sensitive Personal Information:**
  - Personal
    - name, address, dob, contact details etc
  - Sensitive
    - physical, medical and mental health, ethnicity
- **Other Information**
  - If it could be put with some other information a person may have and subsequently identify someone
  - Bank details, key safe codes etc
  - Reasonable expectation that the information will be protected

Information Governance & IT Security: How Could it Go Wrong?

- **Not following Corporate Policies & Standards**
- **Failing to report incidents**
- **Information being:**
  - Disclosed to the wrong people
  - Lost
  - Stolen
  - Disposed of inappropriately or destroyed in error
- **Not telling people their rights:**
  - How their information will be used and shared
  - Obtaining consent; Identifying lawful grounds
  - Failing to support their rights

Think Privacy

Information Governance & IT Security: How Could it Go Wrong?

- **Appropriate Data Processing or Information Sharing Contracts/Agreements**
  - Not having one in place
  - Failing to monitor them
- **Not keeping information accurate and up to date**
- **IT access rights and use of systems/applications**
  - Excessive: edit when read only would suffice, access to shared network drives
  - Used inappropriately/unlawfully
- **Insufficient training**
  - About protecting information
  - On how to use the technology and systems, e.g. Webmail

Think Privacy

Information Governance & IT Security: How Could it Go Wrong?

- **Using unencrypted devices for personal and sensitive personal data**
  - e.g. laptops, memory sticks, magic pens
  - Lost or stolen
  - Used inappropriately and against corporate policy
- **Social networking sites**
  - Inappropriate comments
  - Information leaks
- **Using 'cloud' computing & storage**
  - Would you leave your house keys under the mat?

Think Privacy

Information Governance & IT Security: How Could it Go Wrong?

- **Using an inappropriate method for sending information**
  - e.g. publicly provided email accounts like Yahoo, Hotmail, AOL etc: it's a public post card
  - Wrong fax number
  - Sensitive, valuable documents lost in the post
  - Leaving sensitive information on answer machines, voicemail
- **Not taking into account the sensitivity of the information**
  - And failing to classify it!
- **Failing to quality check**
- **Failing to think about privacy in other processes**
  - Complaints
    - Is the complainant the person who the Information is about?

Think Privacy

Information Governance & IT Security: Examples of What You Need to Do

- **Comply with Corporate policies and standards**
  - Information Security Management
  - Data Protection
  - Standard for Information Classification
  - Standard for ICT Access Control
  - Records Management
  - Reporting Information Incidents
  - Follow your Local Operating Procedures
- **Training and Awareness**
  - Identify & agree with your line manager
  - E-Learning Data Protection etc

Think Privacy

Information Governance & IT Security: Examples of What You Need to Do

- **Promptly report the incident to:**
  - Relevant line manager
  - Information Governance Team (IGT)

- **Provide as much information as possible about:**
  - The information that may have been compromised
  - What happened, when, who
  - What actions have been taken

- **Refer to the 'How to Report an Information Security Breach' for more information**

Think Privacy

Information Governance & IT Security: Examples of What You Need to Do

- **Protecting information from being lost or stolen**
  - Take the minimum amount of information with you
  - Ensure you are authorised to take the information out
  - Don't leave it unattended, e.g. hardcopy or IT equipment in cars, meeting rooms etc
  - If authorised to work from home, safeguard it from those who have no right to know
- **Dispose of information correctly**
  - Check retention schedules (if applicable)
  - Regular housekeeping of emails and file storage areas
  - When a document becomes approved do you need to keep the draft?
  - Secure disposal of classified information
  - Use destruction certificates for business records

Think Privacy

Information Governance & IT Security: Examples of What You Need to Do

- **Information about our clients**
  - Tell them how it will be used etc
  - Understand how it can be used
  - Don't keep information longer than necessary
  - Keep their records up to date
  - **Do not use** it to for checking up on family, friends, colleagues
  - Don't allow yourself to be compromised!

Information Governance & IT Security: Examples of What You Need to Do

- **Sharing information with others**
  - Information sharing agreement
  - Data processing agreement
  - Regularly monitor compliance
  - Know what can be shared with who
  - Only share the minimum amount of information required
  - Share it by the most appropriate secure method

Information Governance & IT Security: Examples of What You Need to Do

- **Good Record Keeping**
  - Only record what is required
  - Anything you record is potentially disclosable
  - Keep to the facts
  - Ensure opinions are based on facts
  - Avoid acronyms – they have to be explained, eg NBOT
  - Don’t keep rough notes, drafts etc any longer than necessary

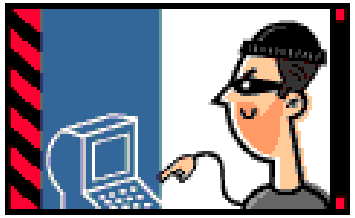
Information Governance & IT Security: Examples of What You Need to Do

- **Use encrypted devices**
  - Council issued only
  - Get authorisation from your manager
  - Safeguard them from being lost, stolen or damaged theft
  - Be familiar with the standard: Management & Use of Removable Media
  - Ensure you know how to use the device correctly
  - Virus check
- **Do not use unencrypted devices for personal/sensitive personal data**

Information Governance & IT Security: Examples of What You Need to Do

IT System Access

- Ensure your access is only sufficient for you to do your job
- **Do not** use it for personal gain (yours or others)
  - Only use it for the purpose for which it was provided
  - Not for snooping on friends, family, colleagues etc
- Check you have the right information, e.g. email address, client record etc
- Safeguard against 'shoulder surfing'
- Do not share log in ids/passwords
- Where necessary, control access to network shared area(s)/folders
- Promptly report errors/unusual activity
- Remember, unlawful use is a criminal offence
  - Personal fine up to £5000 (Magistrates Court)
  - Unlimited at Crown Court



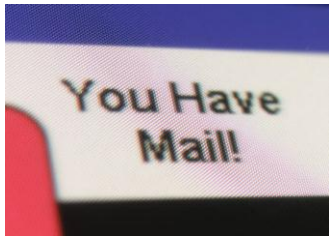
Information Governance & IT Security: Examples of What You Need to Do

- Classifying Information
  - Author of the document
  - Unrestricted: Not worried if it is in the public domain
  - Protect:
    - Short-term inconvenience, harm, distress to one person or organisation
    - Short-term embarrassment to the Council: tomorrow's chip paper!
    - Would not lead to legal, contractual action
  - Restricted:
    - Substantial inconvenience, harm, distress to one or more people/organisations
    - Substantial and sustained embarrassment to the Council and/or public service etc
    - Breach may lead to a fine, prosecution, compensation

If in doubt, refer to the Standard for Information Classification

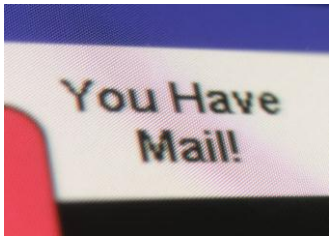
Information Governance & IT Security: Examples of What You Need to Do

- **Email**
  - Council business = Council email account
  - Alternative is Council Webmail **not** personal email accounts
  - Use meaningful subject headers: insert classification as this helps to determine whether it should be sent by email
  - Ensure you have the correct email addresses
  - Only send to those who need to know: don't just reply to all
  - Don't just keep a chain going: create a new message
  - Write it as a business document: what you write may be disclosable
  - Don't type in capital letters
  - Be careful with use of acronyms, punctuation
  - Don't presume the recipient can immediately reply



Information Governance & IT Security: Examples of What You Need to Do?

- **Email**
  - Watch what you attach to emails and calendar events
    - Not everyone may need to know it
  - Proof read it before you send it to make sure:
    - It makes sense
    - It's accurate
    - Spelling and grammar are ok - F7 for spell checker
  - Regular housekeeping
    - Only keep emails for as long as required
    - If it is a required business record, store it correctly eg Shared area
  - Don't circulate junk/spam mail



Information Governance & IT Security: Examples of What You Need to Do

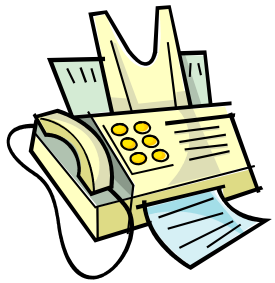
- **Post**
  - Check you have the right address
  - Check you have enclosed the right documents
  - If applicable, mark the envelope eg Personal – Addressee Only
  - If sending sensitive data or a large quantity of personal data, consider more secure means:
    - Special Delivery
    - Collection
    - Courier
  - Refer to Post it Right to ensure you are following the Council's standards for addressing envelopes

Information Governance & IT Security: Examples of What You Need to Do

- **Fax Machines**

  Not ideal for personal and sensitive personal data unless you have controls in place.

  - Make sure that you have the correct fax number
  - If using pre-programmed numbers ensure they are kept up to date
  - Phone ahead to tell the person you are sending them a fax.
    -They may tell you it's not appropriate as they are not in the office
  - Use a fax cover sheet. Include:
    - Who the fax is for? (eg name, title)
    - How many pages you are sending?
  - If the fax has been sent to the wrong person:
    - Immediately contact e.g. A N Other, on 1234567



Information Governance & IT Security: Examples of What You Need to Do

- **Clear Desk Policy**

  Records containing personal data must be:

  - Securely locked away when not in use
  - Not left in print, post and fax trays
  - Ensure personal information displayed on your monitor cannot be viewed by unauthorised people

- **Managing Files**
  - Ensure client records do not get mixed up
  - If moving files around, have a file tracking system in place
  - Refer to your retention and disposal requirements
  - Use file/record destruction certificates

Information Governance & IT Security: Examples of What You Need to Do

- **Scanning**
  - Do not leave ‘scanned documents’ in your ‘scanned drive’
    - Re-file to most appropriate folder etc
    - Delete if no longer needed

- **Printing & Photocopying**
  - Make sure you have selected the right printer
  - Use ‘locked print’ if you are printing sensitive information
  - Promptly collect printing:
    - To stop others from seeing if they have no right to do so
    - To prevent it from getting mixed up with someone else’s printing etc

  - If sending sensitive information to P&F for copying:
    - Ensure it is adequately protected so pages/files are not ‘lost’ or damaged
    - Classify the information
    - Have a process in place to ensure P&F can check that they have received everything sent and vice versa

Information Governance & Security: Some Key Messages

- Information is an important Council asset and keeping it safe secure is the responsibility of us all.
- Ensure you & the Council comply with the Data Protection Act.
- Protect information about people.
- Never use Council information or systems for personal gain.
- Do not share passwords.
- Only use the information for the reason it was provided.
- Use the Council email system for Council business (inc. Webmail)
- Unencrypted storage devices are not safe.
- Promptly report suspected/actual incidents, faults etc.

Information Governance & Security: How Do I Find Out More?

- **Key Contacts**
  - Service Desk ext: 7777, email: servicedesk@coventry.gov.uk for reporting faults & incidents
  - Information Governance Team ext: 3323, email: infogov@coventry.gov.uk or look at IGT Intranet Pages for advice on DPA, FOI and reporting information incidents
  - IT Security ext: 5506, email: ITSecurity@coventry.gov.uk for advice on technical security controls

Information Governance & Security:

Any Questions?

The process..

- Complete the Client information transfer sheet (to be used in all circumstances when an individual living in either a residential, nursing or Housing with Care scheme is transferred to hospital and when individuals are transferred back to a care establishment)
- Prior to transfer the care establishment is required to complete any outstanding detail
- The information should be placed in a sealed labelled envelope marked ‘Protect – Personal Data’ with senders return details on the back
- Hand to West Midlands Ambulance Service, or as an exception fax to the REACT Team (no more than 30 minutes after leaving the care establishment)
- Transfer sheet handed over to nursing staff at hospital, the information will then be attached to the patient notes to follow them throughout their stay at the hospital
- On discharge from the hospital, whether that be from Accident and Emergency or the main hospital the aim is for the transfer sheet to be updated and returned with the patient; however in cases where this does not happen the information will be provided over the telephone by nursing staff/REACT/discharge team

Any Questions?

- Summary of session
- Working together to improve information sharing for the benefit of our clients
- Any questions?

Thank you for attending