NHS
Blood and Transplant

Who Owns What?

New Technologies and their Legal and Practical Implications

Presented by
Kate Holmes BSc PhD LLM
Information Governance Services Manager
22nd May 2013

NHS
Blood and Transplant

Summary

- What is an information asset?
- Can an information asset be owned?
- The impact of new media
- What does this mean in practice?
- Open forum

NHS
Blood and Transplant

Types of Information Asset

- Collections of personal data
  - Clinical databases, bank ledgers ....
- Corporate records
  - Board minutes, contracts, accounts ....
- Intellectual property
  - Inventions, trade secrets, photographs, music ....
- Corporate and personal memory
  - Individuals' knowledge, memory, experience, unrecorded details
- Hardware and software that collect, hold, manipulate, present information

NHS
Blood and Transplant

The Ownership Question – Personal Data

- Personal data belongs to its subjects.
- This means that organisations holding collections of personal data do not own the data, but merely have duties in respect of it.
  - This applies even if the organisation has a legal obligation to collect the data
- It is the data subjects who have rights over their data
- Even ‘Information Asset Owners’ own the responsibility rather than the information itself

NHS
Blood and Transplant

The Ownership Question – Intellectual Property

- Copyright is the protection of the right to benefit from a piece of original work
- It exists automatically, without having to be claimed or labelled
- If copyright is breached, the holder may sue for damages
- Public domain materials such as music, artwork, logos and photographs remain under copyright

NHS
Blood and Transplant

The Ownership Question – Corporate Information

- Contracts of employment normally transfer intellectual property rights to employer
- Even sensitive information such as security details or investigation reports are more ‘held’ than ‘owned’
- Facts cannot be owned per se
- The challenge is to enable efficient appropriate sharing of relevant information while protecting and withholding sensitive material

NHS
Blood and Transplant

The Internet and Beyond

- Web presence is essential in 21st Century
- Very powerful outward communication tool
- Structure and content must be managed carefully
- Inbound communication by web forms has high user uptake but beware:
  - Cannot prevent inappropriate use e.g. wrong form, sensitive content, rejection of Ts and Cs, need for identifiability versus privacy, etc.

NHS
Blood and Transplant

Cloud Computing

- Software as a Service ('SaaS') can offer huge savings over traditional model of purchasing hardware, software and data storage capacity and employing people to run it;
- All clouds are not alike!
  - Can be private, public, community or hybrid. Even public cloud can offer higher security than some traditional systems
- Remember your Data Controller obligations, specify your requirements very clearly and ensure supplier is ready to meet them

NHS
Blood and Transplant

DPA Principles Require:

- Fair and lawful processing
- Stated purpose(s)
- Adequate, relevant, not excessive data
- Accurate and up to date data
- No obsolete data
- Compliance with data subjects' rights
- Security
- No overseas transfer unless equivalent rights and protections guaranteed

NHS
Blood and Transplant

Security Considerations

- Processor contracts
  - Hosting organisations, Cloud providers, Software as a Service (SaaS)
- Data transfer
  - Security such as encryption in place end to end
- Link to Eighth Principle
  - www means World Wide Web!
  - Restrictions on data storage for SaaS providers

NHS
Blood and Transplant

Social Media

Information Governance

NHS
Blood and Transplant

The Benefits of Communication by Social Media

- Speed
- Cost
- Easy two-way communication
- Multimedia
- Wide coverage
- Potential for further sharing
- Ongoing availability
- Attractiveness and accessibility

NHS
Blood and Transplant

The Risks of Communication by Social Media

- Speed
- Cost
- Easy two-way communication
- Multimedia
- Wide coverage
- Potential for further sharing
- Ongoing availability
- Attractiveness and accessibility

NHS
Blood and Transplant

Blurring the Boundaries – Corporate and Personal Use of Social Media

- Impossible to prevent employees using personal accounts and hardware during breaks
- Nonsensical to continue blocking access to media when NHSBT uses Facebook and Twitter for its own business purposes
- Link to Code of Conduct
  - behaviour likely to bring NHSBT into disrepute
  - Misuse of work time
- Official guidance for those whose job it is to run the accounts – language, tone, content, moderation
- Safe and appropriate use guidance for all staff in mandatory training

NHS
Blood and Transplant

Advice covers:

- Privacy and reputational risks
  - Tribunal finding ‘no expectation of privacy’
  - Unclear and changing account terms
- Durability of posts, incl. by sharing and repeating
- Identity theft and personal security
- Social engineering for anti-corporate malicious purposes
- Corporate responsibility, including reminder of appropriate channels for whistleblowing

NHS
Blood and Transplant

Data Leakage Prevention

- Newly arrived in NHSBT
- Applies to corporate e-mail, social media, webmail, web forms
- Uses ‘rules’ to identify if content may be sensitive, e.g. large numbers of names, 10-digit numbers, trigger words
- Can report in stealth mode, report to sender and allow choice, or block completely
- Needs considerable customisation for effective deployment

NHS
Blood and Transplant

Questions?