Legalities of Data Protection, Confidentiality & data flows/storage

UNIVERSITY of DERBY

www.derby.ac.uk

Introduction

- Quick common sense overview of
  - Information Confidentiality
  - Data protection on email & data storage
  - In 20 minutes

What does it "look" like?

how confidential/sensitive is it?

Source: http://www.nsai.ie/Images/Standards-Images/STD-SIS-InformationLW.aspx

The Duck Test

If it walks like a duck & quacks like a duck then it's probably a duck

How to identify confidential data

- "First, the information must itself … have the necessary quality of confidence about it.
- Secondly, that information must have been imparted in circumstances importing an obligation of confidence.
- Thirdly, there must be an unauthorised use of that information to the detriment of the party communicating it."

Source Megarry J, COCO V. A.N. CLARK (ENGINEERS) LTD [1969] RPC 41

Strict Confidentiality

- NHS term

- Likely based around ECHR 2009/14 case of Szuluk v. the United Kingdom, 2 June 2009. A prisoner had medical correspondence to his consultant intercepted and read by the prison medical officer. UK courts agreed with this but the ECHR disagreed.

- If this was e-mail, then the attachment or email must be encrypted (i.e. making plain text impossible to read without a password or key)

- http://www.nhsla.com/claims/Documents/Hill%20Dickinson%20Health%20insights%20-%20The%20importance%20of%20confidential%20correspondence%20between%20doctors%20and%20prisoners.pdf

Where is the data & how secured?

- Data has 2 states
  - At rest (on a server, in email etc)
  - In transit (email in motion, upload/download)

- Both states need thinking about & securing

Statute Law

- Access to Health Records Act (1990)
- The Human Rights Act (1998)
  - …The right to respect for his private and family life, his home and his correspondence.
- EU Data Protection Directive 95/46/EC led to the Data Protection Act (1998).
    - N.B Only applies to living people
- General Data Protection Regulation 2018
  - Update for the digital age, stricter than previously

Checklist (1)

1. What data needs to be sent & how?
2. How will it be secured in motion, if needed?
3. How will it be secured at rest, if needed?
4. What contracts are in place?
    1. Standard, i.e. t's & c's?
    2. Bespoke - i.e written contract

Checklist (2)

5. Whose law applies? - yes, read the t's & c's!

6. Where are the systems located ?

7. How are they secured?

Where is your data?

Let's follow an email

- Written in Outlook (at rest)
- Sent (in motion) as it goes through various email servers
- Arrives on destination system (at rest)
- Collected - in motion then at rest again

Now lets think about the data just sent

- A calling notice for a LEN meeting
- An email about someone's sickness absence
- a list of disabled people and their disabilities and treatments

Other points to note

- Shared assumptions usually aren't!
  - Think about emails between staff, students, carers - need for clear signposting of what's expected
  - Good enough security vs beyond doubt
    - What needs encryption?
    - whose risk?