National Data Guardian

Governance in Shared Record Systems

SCIMP & SNUG Conference 2016

Wednesday 21 September 2016

Dr Alan Hassey

Governance: security

- National Data Guardian in England has proposed ten new data security standards
- Ten standards are grouped under three themes – people, processes, technology
- Leaders are called on to take responsibility for them
- Designed to be applicable to range of organisations from small GP practice or care organisation to large hospital trust

National
Data
Guardian

Leadership Obligation 1: People

Leadership Obligation 1: People: Ensure staff are equipped to handle information respectfully and safely, according to the Caldicott Principles.

Data Security Standard 1. All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is only shared for lawful and appropriate purposes

Data Security Standard 2. All staff understand their responsibilities under the National Data Guardian's Data Security Standards, including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.

Data Security Standard 3. All staff complete appropriate annual data security training and pass a mandatory test, provided through the revised Information Governance Toolkit.

National
Data
Guardian

Leadership Obligation 2: Process

Leadership Obligation 2: Process: Ensure the organisation proactively prevents data security breaches and responds appropriately to incidents or near misses.

Data Security Standard 4. Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access to personal confidential data on IT systems can be attributed to individuals.

Data Security Standard 5. Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security.

Data Security Standard 6. Cyber-attacks against services are identified and resisted and CareCERT security advice is responded to. Action is taken immediately following a data breach or a near miss, with a report made to senior management within 12 hours of detection.

Data Security Standard 7. A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report to senior management

National Data Guardian

Leadership Obligation 3: Technology

Leadership Obligation 3: Technology: Ensure technology is secure and up-to-date.

Data Security Standard 8. No unsupported operating systems, software or internet browsers are used within the IT estate.

Data Security Standard 9. A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually.

Data Security Standard 10. IT suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardian's Data Security Standards.

National
Data
Guardian

Opt-out

The NHS Constitution says

You have the right to be informed about how your information is used.

You have the right to request that your confidential information is not used beyond your own care and treatment and to have your objections considered, and where your wishes cannot be followed, to be told the reasons including the legal basis.

National
Data
Guardian

Consent for record sharing

- Where record sharing is solely for direct care – consent might be implied
- Must be a legitimate relationship with the patient
- Some models rely on implied consent with explicit consent for access at the point of care
- Emerging models may require higher degree of patient participation to get professional buy-in and realise benefits
- Data controller responsibilities – are the right agreements and safeguards in place?
- No surprises

National
Data
Guardian

Questions and discussion

National
Data
Guardian