The National Data Security Review
Assuring Leadership:
Developing the role of the SIRO and Caldicott Guardian

Christopher Fincken
Chairman UK Caldicott Guardian Council (2012-2017)
A Caldicott Guardian for Marie Curie
The National Data Guardian’s data security standards

These standards are intended to apply to every organisation handling health and social care information, although the way that they apply will vary according to the type and size of organisation.

Leaders of all health and social care organisations should commit to the following data security standards. They should demonstrate this through audit or objective assurance, and ensure that audit enables inspection by the relevant regulator.
The Health & Social Care “System”  
(some of it!)

• 160 Acute Trusts
• 56 Mental Health Trusts
• 34 Community Providers
• 24 Ambulance Trusts
• 211 CCGs
• 34 NHS England Area Teams
• 152 Councils with Adult Social Care Responsibilities (CASSRs)/providers of Local Public Health Teams
• 8,230 GP practices
• 20,100 registered Care Homes
• 6,830 registered Care Agencies

©C. Fincken 2015
“The first duty of government is the protection of life, not its destruction. Abandon that, and you have abandoned all.”

Attributed to Thomas Jefferson
Data security Recommendation 1:

The leadership of every organisation should demonstrate clear ownership and responsibility for data security, just as it does for clinical and financial management and accountability.
What is Leadership?
• The CEO and Board
• The Caldicott Guardian (CG)
• The Senior Information Risk Owner (SIRO)
• Who Else?

SILOS
The Leader Within

- Authority
CALDICOTT GUARDIAN
(Deputies?)

SIRO

IG TEAM
DIFFERENCE BETWEEN CALDICOTT AND IG

SIRO’s and Caldicott Guardians
SECURITY AND IG ARE NOT NEW!
Cyber Security

Isn’t Security “IG” not Caldicott?

Not Just IG! Caldicott Guardians need to be involved. When are patients to be told about breaches?

Not Just Cyber!
Caldicott Guardians bring to bear ethical as well as legal considerations, making fine judgements about human situations that are rarely codified and could not be done by a machine.
WEBSITE MANUAL COMING SOON

https://www.gov.uk/government/groups/uk-caldicott-guardian-council

The Secretariat can be contacted via email: ukcgcsecretariat@nhs.net
THE CAPTAIN
THE CREW
THE PASSENGERS

Have You washed your hands?
2.4.2 Staff behaviour was often cited as the unintentional cause of breaches, with ‘simple errors, often compounded by heavy workloads, unclear or badly implemented policies and procedures. Mostly they can be described as naivety rather than deliberate non-compliance’

34. The human element is considered one of the most relevant threat factors and should be mitigated through tailored training for all staff.
2.4.4 When considering what could help to address behavioural issues, consistent training, education and awareness emerged as being vital. As also found in Caldicott2, this was considered essential to addressing the culture of risk aversion, often resulting from a lack of confidence in security capability by senior management. Leaders should address cultural barriers by proactively engaging staff and involving national workforce organisations to support professional capability in this area.
Implementing the leadership obligations outlined in the national review
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.
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.
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 Standard.
Ensuring Staff are equipped to handle information respectfully and safely according to the Caldicott Principles
Caldicott Principles (revised 2013)

1. Justify the purpose(s)
Caldicott Principles

2. Don’t use personal confidential data unless it is absolutely necessary.
Caldicott Principles

3. Use the minimum necessary personal confidential data
Caldicott Principles

4. Access to personal confidential data should be on a strict need-to-know basis
Caldicott Principles

5. Everyone with access to personal confidential data should be aware of their responsibilities.
Caldicott Principles (revised 2013)

6. Comply with the law
DATA PROTECTION ACT 1998

PRINCIPLE 7.
Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
Caldicott Principles (revised 2013
7. The duty to share information can be as important as the duty to protect patient confidentiality. Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.
How do we ensure all staff complete mandatory data security training and pass a mandatory test?
So How do we do it?
How can you get everyone on board?

Christopher Fincken
07891 641090
caldicottguardian@ hotmail.co.uk
(Non Secure!)