CSC

The Northern, Yorkshire and Humberside NHS Directors of Informatics Forum
www.nyhdif.org.uk
NYHDIF
Improving patient care by sharing ideas and information

Healthcare Cyber Security – Secure, Vigilant and Resilient

Stu Brett
Aaron Chatfield
November 2016

Secure, Vigilant and Resilient

1. Cyber Security? Why Bother?
2. NHS Cyber Security in the News
3. The Threats You Face
4. What Can be Done About it?
5. People, Process & Technology
6. What Help is Out There?
7. Simple Takeaways

Cyber Security? Why Bother?

INFORMATION
to share or
not to share

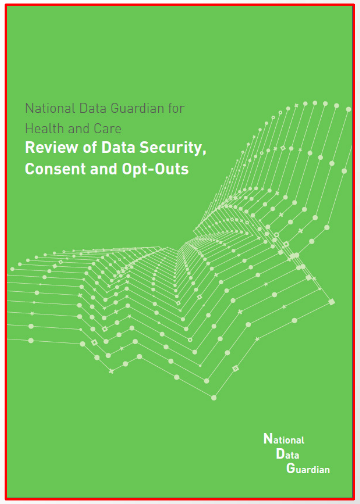
The Information Governance Review

Caldicott Report 1997 and Information Governance Review 2013

1. Justify the purpose
2. Don’t use personal confidential data unless it is absolutely necessary
3. Use the minimum necessary personal confidential data
4. Access to personal confidential data should be on a strict need-to-know basis
5. Everyone with access to personal confidential data should be aware of their responsibilities
6. Comply with the law
7. The duty to share information can be as important as the duty to protect patient confidentiality

Review of Data Security, Consent and Opt-Outs – June 2016

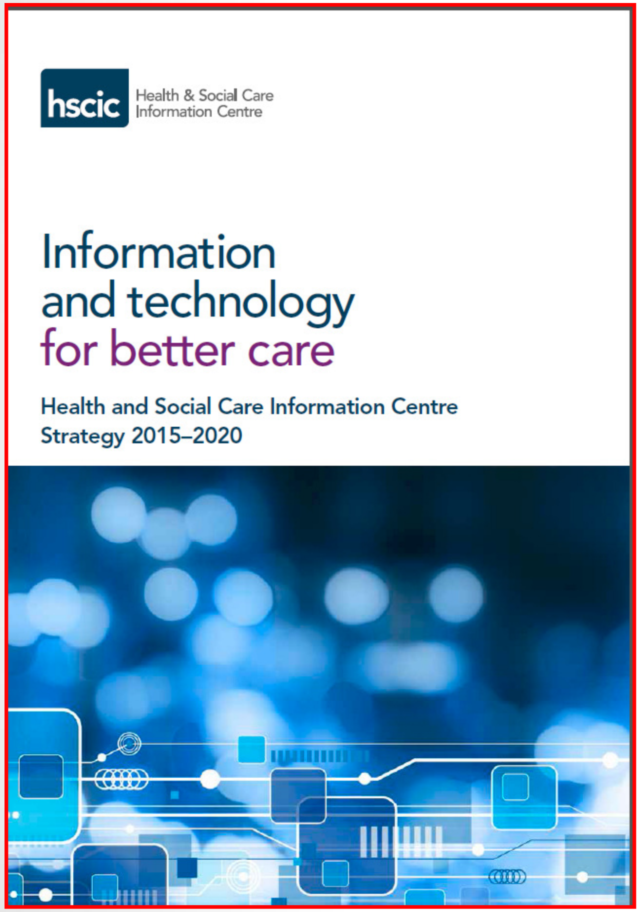
- “Whilst there are examples of good practice and most organisations are concerned about data security, there are problems involving people, processes and technology.....”
- “Personal confidential data is valuable to those with malicious intent, and health and social care systems are will continue to be at risk of external threats and potential breaches. However, internally, data breaches are often caused by people who are finding workarounds to burdensome processes and outdated technology, and may have a lack of awareness of their responsibilities…”



National Data Guardian for
Health and Care
Review of Data Security,
Consent and Opt-Outs

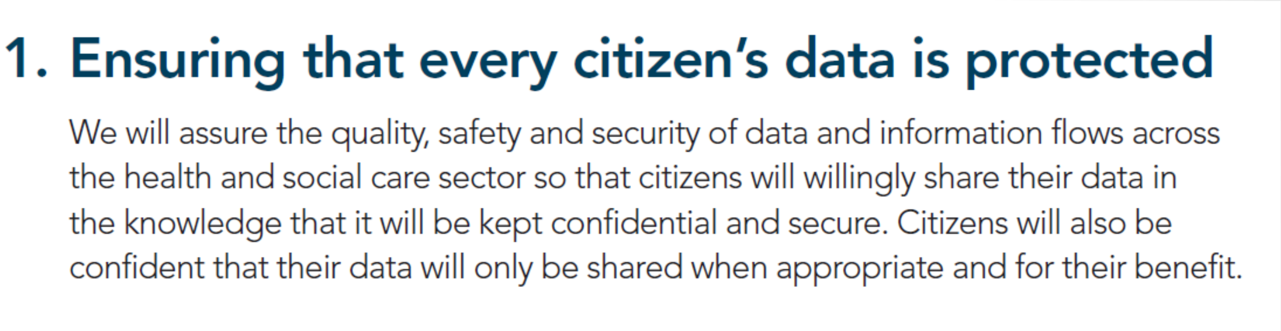
National
Data
Guardian

Cyber Security? Why Bother?

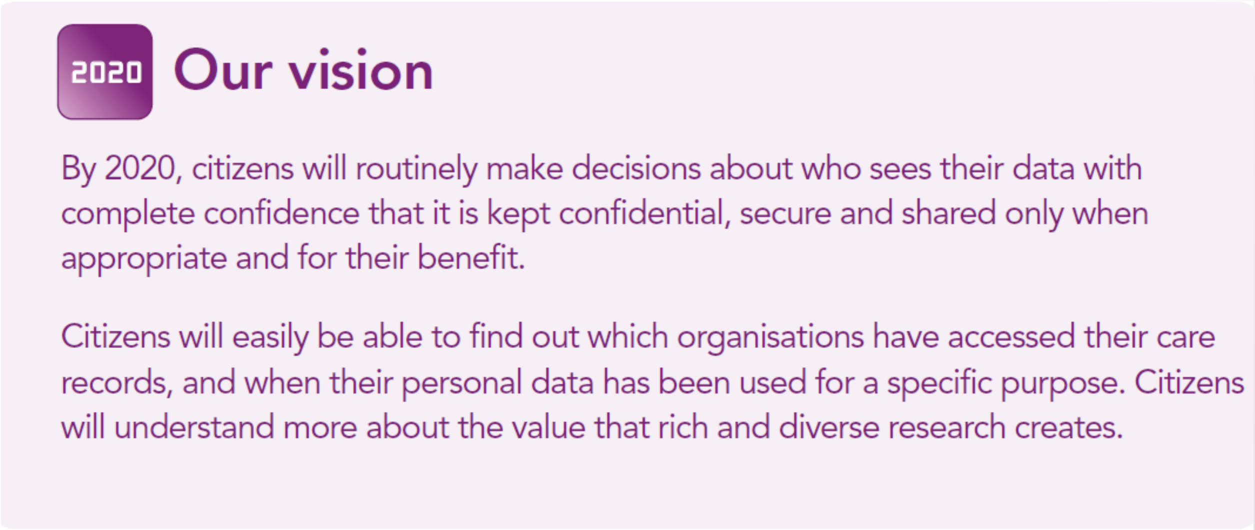

hscic Health & Social Care Information Centre

Information and technology for better care

Health and Social Care Information Centre Strategy 2015–2020


1. Ensuring that every citizen's data is protected

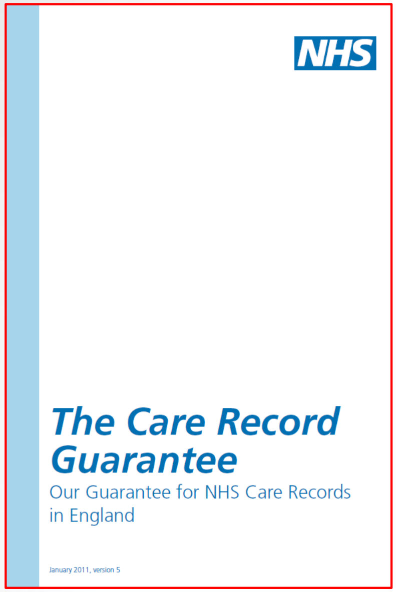
We will assure the quality, safety and security of data and information flows across the health and social care sector so that citizens will willingly share their data in the knowledge that it will be kept confidential and secure. Citizens will also be confident that their data will only be shared when appropriate and for their benefit.


2020 Our vision

By 2020, citizens will routinely make decisions about who sees their data with complete confidence that it is kept confidential, secure and shared only when appropriate and for their benefit.

Citizens will easily be able to find out which organisations have accessed their care records, and when their personal data has been used for a specific purpose. Citizens will understand more about the value that rich and diverse research creates.

Cyber Security? Why Bother?



NHS

The Care Record Guarantee

Our Guarantee for NHS Care Records in England

January 2011, version 5

The Care Record Guarantee 2011

10. We will take appropriate steps to make sure we hold records about you – both paper and electronic – securely and only make them available to people who have a right to see them.

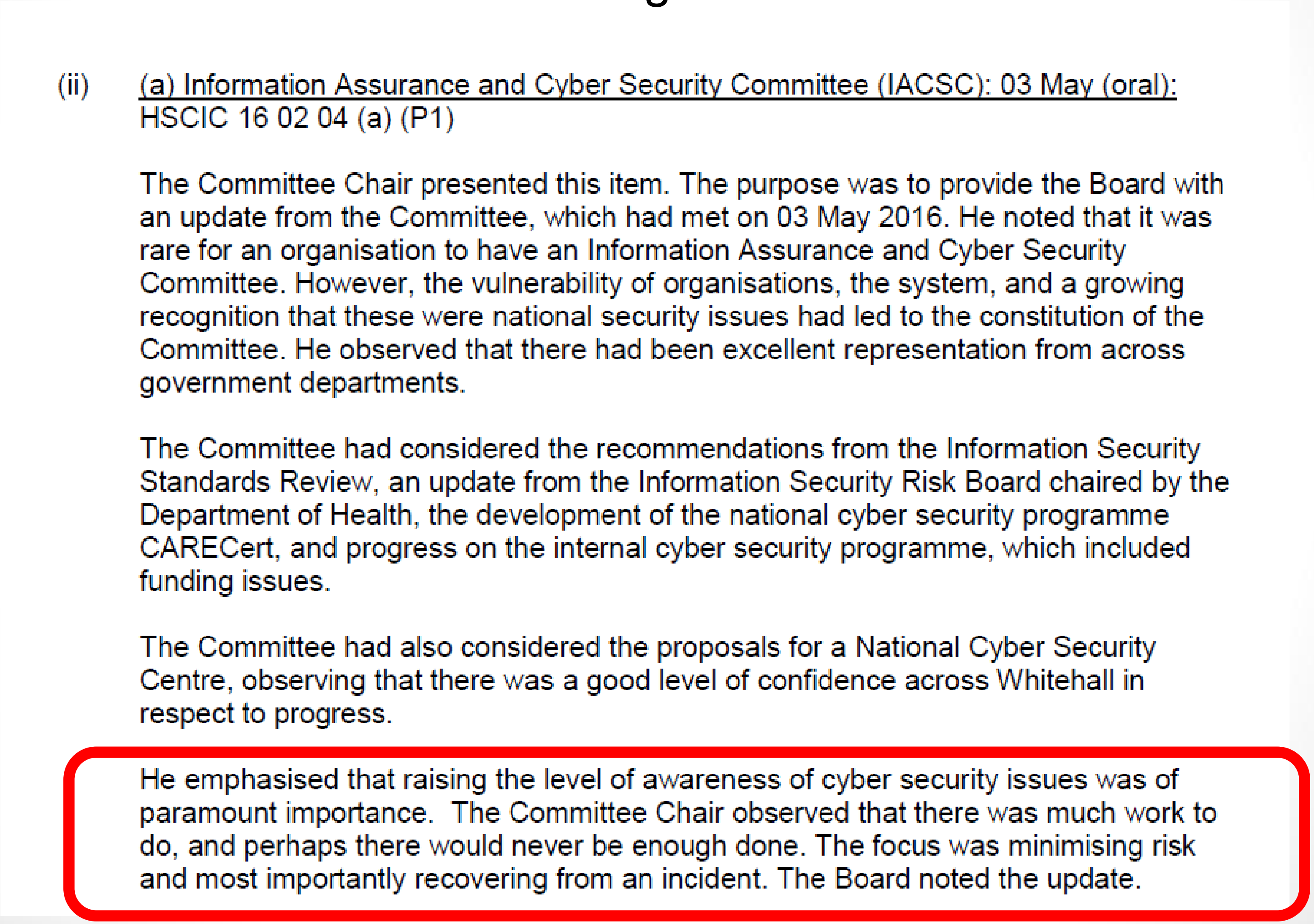
11. We will keep a record in the newer electronic record systems of anyone who has accessed a health record or added notes to it. Some of the older computer systems will only record who has accessed a record where they have made changes.

EU General Data Protection Regulation

- Ratified in May 2016, EU nations obligated to apply it by May 2018
- UK PM stated on 2nd Oct 2016 that Government will incorporate all existing EU laws into UK law and then trigger Article 50 by April 2017.
- UK will still need to prove ‘adequacy’ in its data protection laws if we wish to trade with the Single Market, equivalent to GDPR, in 2018
- Changes to consent, breach notifications, 3rd party processing responsibilities, and significantly increased fines (up to €20M)

Cyber Security? Why Bother?

Minutes of the HSCIC Board meeting – 8th June 2016



(ii) (a) Information Assurance and Cyber Security Committee (IACSC): 03 May (oral): HSCIC 16 02 04 (a) (P1)

The Committee Chair presented this item. The purpose was to provide the Board with an update from the Committee, which had met on 03 May 2016. He noted that it was rare for an organisation to have an Information Assurance and Cyber Security Committee. However, the vulnerability of organisations, the system, and a growing recognition that these were national security issues had led to the constitution of the Committee. He observed that there had been excellent representation from across government departments.

The Committee had considered the recommendations from the Information Security Standards Review, an update from the Information Security Risk Board chaired by the Department of Health, the development of the national cyber security programme CARECert, and progress on the internal cyber security programme, which included funding issues.

The Committee had also considered the proposals for a National Cyber Security Centre, observing that there was a good level of confidence across Whitehall in respect to progress.

He emphasised that raising the level of awareness of cyber security issues was of paramount importance. The Committee Chair observed that there was much work to do, and perhaps there would never be enough done. The focus was minimising risk and most importantly recovering from an incident. The Board noted the update.

NHS Cyber Security in the News

“The NHS is at risk of cyber attacks, a minister warns today as he says that hacking is “no longer the stuff of spy thrillers and action movies" but a clear and present threat.”

The Daily Telegraph, 31st Oct 2016

Northern Lincolnshire and Goole NHS Foundation Trust (NLAG) said systems were infected with a virus on Sunday, with it treated as a "major incident"

BBC, 1st Nov 2016

“The NHS is under frequent cyber attack, with a national attack that “may or may not” have been state sponsored having been launched just this month.”

NHS Digital COO, 28th Sept 2016

The Threats You Face

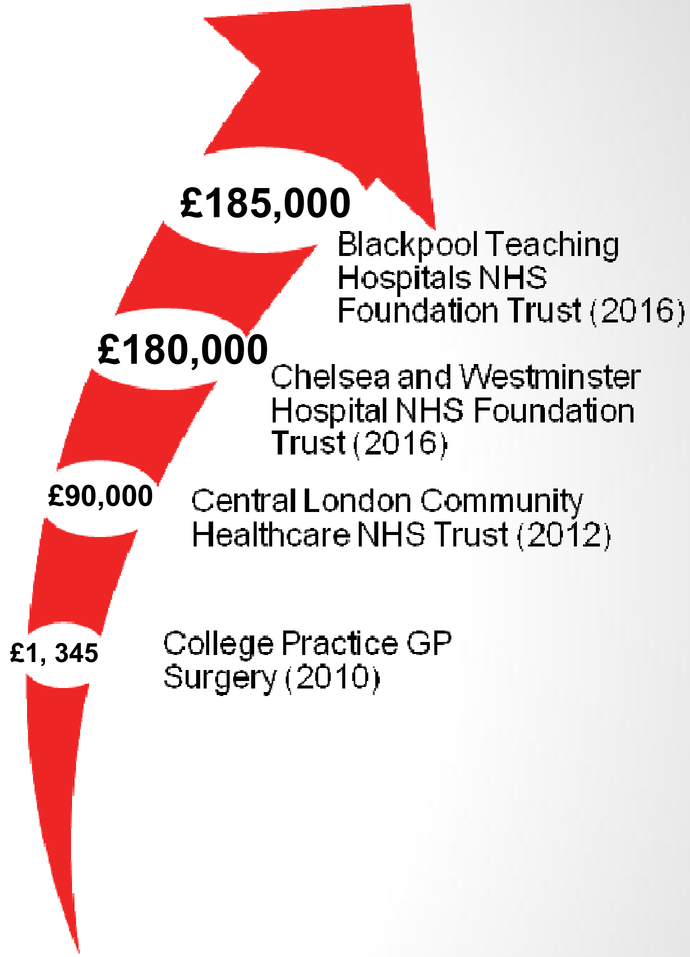
- External
  - Ransomware attacks doubled in 2015
  - The number of new ransomware variants increased 17% in Q1 2016
  - Attackers after personal data
- Internal
  - Move to electronic records
  - Retention of old paper records
  - Digitisation of patient services
  - Technology-enabled patient care
  - Lack of basic cyber security training and awareness
    - Keeping passwords safe
    - Never letting anyone else use a Smartcard
    - Not clicking on unverified links in emails
    - Keeping mobile devices safe and secure
    - Log off or lock screens when not in use
  - Understanding of personal responsibility to keep data safe

Health Sector Breaches

43% of ALL data breaches come from the Health Sector

47% of NHS Trusts subject to ransomware attack in last year

- Over the 2011 – 2014 period there were **7255** data breaches within the health sector, the equivalent of **6** breaches a day
- In 2015 **112 Million** records were lost from Healthcare Organisations



£185,000 Blackpool Teaching Hospitals NHS Foundation Trust (2016)

£180,000 Chelsea and Westminster Hospital NHS Foundation Trust (2016)

£90,000 Central London Community Healthcare NHS Trust (2012)

£1, 345 College Practice GP Surgery (2010)

81% Health sector data breaches increased from 14/15 to 15/16 FY

1.3M Total amount of fines levied on the NHS from the ICO

As of 2015, Healthcare is now the most frequently attacked industry, surpassing both Financial services and Manufacturing

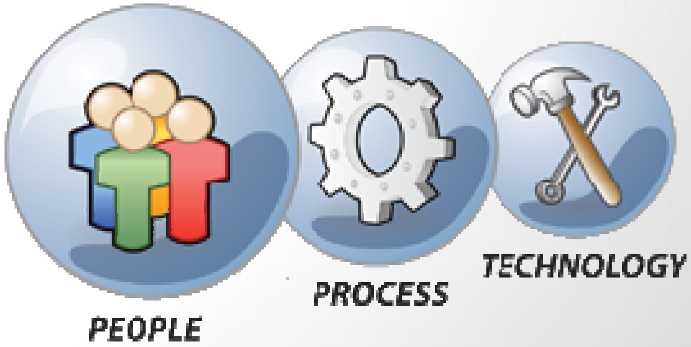
References: ICO, Big Brother Watch Report 2014, Office of Civil Rights.

What Can be Done About it?

- Balance of risk vs control
- Understand what you want to protect
  - Patient clinical data
  - Staff employee records
- What would happen if you lost this data?
  - Risk based approach
- How much do I need to spend?
  - Cost Benefit Analysis based on your appetite to risk
- Look at your People, Process and Technology

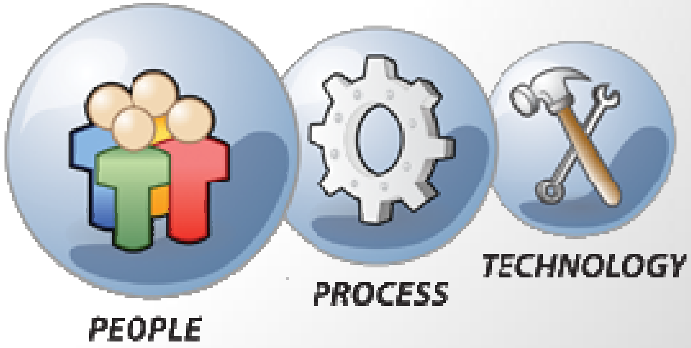
People

- Is there a member of staff with formal responsibilities for cyber security?
- Does cyber security lead know how the organisation operates, do they engage with the business and know where to prioritise effort?
- Are there sufficient number of skilled cyber security staff with relevant industry experience focused on the right areas?
- What is the cyber security culture like – is cyber security risk considered across all activities in the organisation?
- Is there an organisation-wide education and awareness campaign established around cyber security?
- Is physical security appropriate to protect what needs to be protected?



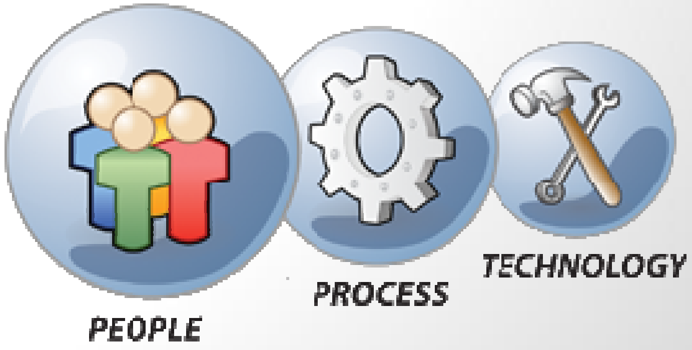
Process

- Is there a clearly articulated risk appetite and are cyber security risks incorporated into existing risk management and governance processes?
- Are cyber security risk discussions elevated to the board level?
- Is there an enterprise-wide cyber security policy approved by the board, with clear roles and responsibilities?
- Do you adopt an industry framework to establish, operate and maintain your cyber security program (ISO 27001, CIS Critical Security Controls, Cyber Essentials)?
- Is there an cyber security incident management framework in place, is this integrated with existing business continuity management and disaster recovery plans? Is it ever tested?
- How about your suppliers, are processes in place to ensure they align to your cyber security requirements?

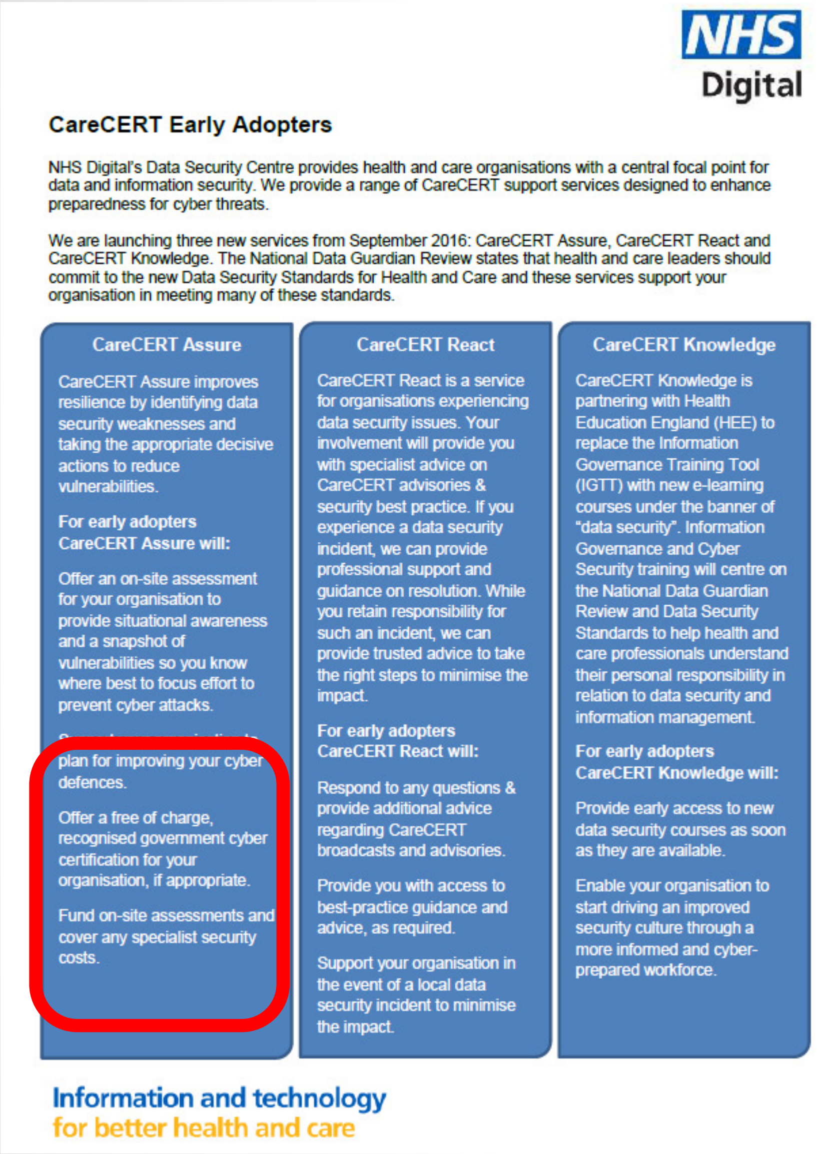


Technology

- Operations security
  - What is on your network (hardware and software)?
  - Threat vulnerabilities and proactive monitoring
  - Email and malware
  - Encryption/Secure VPNs
- Network Security
  - Boundary protection
  - Device protection
  - Segmentation
- Controlling Access
  - Who is accessing what, and when?
  - How do you know, are these the correct access controls?
  - Privileged user access management



What Help is Out There?



NHS Digital

CareCERT Early Adopters

NHS Digital's Data Security Centre provides health and care organisations with a central focal point for data and information security. We provide a range of CareCERT support services designed to enhance preparedness for cyber threats.

We are launching three new services from September 2016: CareCERT Assure, CareCERT React and CareCERT Knowledge. The National Data Guardian Review states that health and care leaders should commit to the new Data Security Standards for Health and Care and these services support your organisation in meeting many of these standards.

CareCERT Assure

CareCERT Assure improves resilience by identifying data security weaknesses and taking the appropriate decisive actions to reduce vulnerabilities.

For early adopters CareCERT Assure will:

Offer an on-site assessment for your organisation to provide situational awareness and a snapshot of vulnerabilities so you know where best to focus effort to prevent cyber attacks.

Support your organisation to plan for improving your cyber defences.

Offer a free of charge, recognised government cyber certification for your organisation, if appropriate.

Fund on-site assessments and cover any specialist security costs.

CareCERT React

CareCERT React is a service for organisations experiencing data security issues. Your involvement will provide you with specialist advice on CareCERT advisories & security best practice. If you experience a data security incident, we can provide professional support and guidance on resolution. While you retain responsibility for such an incident, we can provide trusted advice to take the right steps to minimise the impact.

For early adopters CareCERT React will:

Respond to any questions & provide additional advice regarding CareCERT broadcasts and advisories.

Provide you with access to best-practice guidance and advice, as required.

Support your organisation in the event of a local data security incident to minimise the impact.

CareCERT Knowledge

CareCERT Knowledge is partnering with Health Education England (HEE) to replace the Information Governance Training Tool (IGTT) with new e-learning courses under the banner of "data security". Information Governance and Cyber Security training will centre on the National Data Guardian Review and Data Security Standards to help health and care professionals understand their personal responsibility in relation to data security and information management.

For early adopters CareCERT Knowledge will:

Provide early access to new data security courses as soon as they are available.

Enable your organisation to start driving an improved security culture through a more informed and cyber-prepared workforce.

Information and technology
for better health and care

CareCERT

- Funding from the Cabinet Office National Cyber Security programme
- "*enhance cyber resilience across the health and social care system*"
- NDG to draw up new protocols against which CQC can inspect against (~April 2017)
- NHS Digital to issue cyber security alerts on a monthly, weekly and even daily basis, including, where possible, information on how organisations should deal with specific attacks
- Beta testing a national cyber security training platform; basic level for all staff and a more complex module for specialist staff

Simple Takeaways to Improve Your Security Posture

1. Locate your ‘crown jewels’ and prioritise their protection
2. Talking is good – raise awareness of common cyber security issues amongst staff, such as phishing attacks and social engineering
3. Back up your data – don’t be a ransomware victim!
4. Patch regularly – attackers exploit known vulnerabilities
5. Understand in detail what the entire business needs to do in the event that something goes wrong – hope is not a strategy…

"Security starts on the frontline, not in the IT department"

Dan Taylor, Head of Cyber Security, NHS Digital – 11th July 2016