# Customer Compliance and Cyber Security

Information and technology
for better health and care

Paul Evans

# What we are doing

- *Introducing a Connection Agreement for HSCN to replace the IGSoc for N3*
- *Separating getting hooked up to the network from data security*
- *Focusing on wider data and cyber security through a collaborative approach*
- *Introducing network traffic analysis:*
- *Retaining internet gateway content checking and malware filtering*

# Why we are doing it


The HSCN is an enabler


Proportional security compliance


Data security - the threat of malware

# HSCN Connection Agreement – Key Points

| | |
|---|---|
| What is it? | Sets out the things customers must do |
| Who completes one? | Every organisation that uses the HSCN |
| When is it completed? | Before CN-SP can connect |
| Is it completed annually? | No, but some details need to be kept up to date |
| Who needs to sign it? | Executive, Senior Partner, Caldicott Guardian |
| Where is it completed? | On-line |

# Data and Cyber Security

- The network does not secure data, systems or applications….nor does it verify the security quality of any user or end-point…(N3 doesn't either)

- There will be content filtering at the internet boundary……
  - To replicate what is currently there in N3
- …..And network traffic monitoring
  - To help protect the network's own availability and improve cyber across the HSCN community

- NHS Digital are not taking away security requirements for accessing data, systems, applications or services

  - So, as an example, to get access to NHS Digital's National Applications, you will still need to go through those compliance arrangements (currently IGT)

  - For National Applications – and possibly more widely- data security requirements and arrangements will change as a result of the National Data Guardian report towards a one size doesn't fit all