European Partnership for Supervisory Organisations in Health Services and Social Care

Status: ***DRAFT DISCUSSION DOCUMENT*** *to be completed by the members of the working group and third parties invited to do so.*

Introduction to an EPSO – Blueprint for cyber security in healthcare

With the widening use of technology in healthcare, it is important that both providers of healthcare and those organizations with supervisory responsibility take all reasonable steps to ensure their systems are protected from cyber attack. This document is intended to provide information, advice, and guidance to all those in the healthcare sector on how to protect their systems.

Definition of cyber security

The UK National Cyber Security Centre defines as Cyber security as how individuals and organisations reduce the risk of cyber-attack.

Cyber security's core function is to protect the devices we all use (smartphones, laptops, tablets and computers), and the services we access - both online and at work - from theft or damage.

It's also about preventing unauthorised access to the vast amounts of personal information we store on these devices, and online.

Cyber security is important because smartphones, computers and the internet are now such a fundamental part of modern life , that it's difficult to imagine how we'd function without them. From online banking and shopping, to email and social media, it's more important than ever to take steps that can prevent cyber criminals getting hold of our accounts, data, and devices.

Checklist of cyber security considerations

- ❑ Identify your critical systems
- ❑ Ensure your critical systems have an ‘off-line’ back up.
- ❑ What ‘cyber-links’ do you have with partners and how to contact them
- ❑ Have documented contingency plans on paper
- ❑ Have an alternative means of communications separate from organizational network
- ❑ Deliver appropriate cyber security training for all staff
- ❑ Review and examine systems to establish if organizational hacking or unusual activities can be identified.
- ❑ Do not have all systems centralized, split them over a number of separate systems
- ❑ Consider how you will react to demands of cyber criminals (to pay or not pay any ransom demands)
- ❑ Do not restart system after being hacked – to preserve the evidence and trace criminals.
- ❑ Immediately engage highest level of support from professionals and police – do not try and handle alone

- ❑ Consider in advance how you intend to manage publicity regarding the incident and how this will influence the relationship with the criminals
- ❑ Obtain a national accreditation in cyber security preparedness

National support resources

Nation	Resource	Website
Scotland	Scottish Business Resilience centre	Home - Scottish Business Resilience Centre (sbrcentre.co.uk)
UK	Cyber Essentials scheme	Cyber Essentials Scheme: overview - GOV.UK (www.gov.uk)
UK	The National Cyber Secuity Centre	National Cyber Security Centre - NCSC.GOV.UK