
CYBER AWARE

skillsforcare

Local
Government
Association



1. FOREWORD

Thank you for taking the time to read this guidance, which has been produced for Care Providers and for anyone else who would find it of assistance.

It was written by the Care Provider Alliance in collaboration with the Social Care Programme at NHS Digital, with significant contributions from many other agencies including the Home Office (Cyber Aware Team) and the National Cyber Security Centre. The guidance can be found on the Care Provider Alliance website.

For extra information about cyber security, the guidance includes links to web pages from Government approved organisations. They also contain important information about other areas such as: The Data Security and Protection Toolkit (replacing the existing Information Governance Toolkit April 2018) and GDPR (applies from 25th May 2018). Please see **'5. Resource Library'** for more details.

If you have feedback about the websites used in this guidance, please contact the organisation concerned.

2. TECHNOLOGY AND BENEFITS

There are fantastic benefits to embracing technology and working securely online in health and social care. Technology allows greater and faster information sharing, so we can improve the quality of care and support which we provide e.g. personalised care planning, transfers of care, viewing medications, etc. Individuals can fully participate and have better access to, and input into, their records.

However, as we use technology more, we must continue to do all we can to keep data safe and secure, ensuring that disruption to care and support at best is avoided or that any disruption is minimised.

The global ransomware attack in May 2017, which in the UK particw , wh Ġ

3. WHAT IS CYBER SECURITY?

Cyber security is the name for the safeguards taken to avoid or reduce any disruption from an attack on data, computers or mobile devices.

Cyber security covers not only safeguarding confidentiality and privacy, but also the availability and integrity of data, both of which are vital for the quality and safety of care.

Security breaches can occur when we use paper records, send information using fax machines and even verbally. However, the consequences of security breaches with digital information are potentially far more severe, as information can be distributed more easily and to a far wider audience.

Cyber-breaches are costly – in terms of expense, recovery time and through damage to reputation. In a Government Cyber Breaches Survey in 2017, 46% of businesses reported a cyber-breach or attack.

That is why cyber security is a high priority for business and why all staff must be aware of how to implement protective measures.

Individuals should also be aware of basic cyber security safeguards for personal use and when participating in the management and coordination of their care and support.

4. IMPROVING CYBER SECURITY

Cyber security is a constantly changing area and sometimes can seem quite confusing.

However, there are many effective and relatively simple steps that can be taken to protect information and protect you and your organisation.

Taking some simple actions and practising safe behaviours will reduce online threats.

The most important steps to improve online security are ensuring you:

a. MOVE AWAY FROM USING UNSUPPORTED SOFTWARE

This is when software e.g. operating systems such as Windows, apps, web browsers, etc. are no longer updated by the supplier. Although

c. RUN UP-TO-DATE ANTI-VIRUS SOFTWARE

Your computers, tablets and smartphones can easily become infected by small pieces of software known as malware. Common types include viruses or spyware and ransomware. To help prevent infection, install internet security software, like anti-virus and/or anti-malware on your devices and keep it up to date.

For more information, please click here.

d. USE STRONG PASSWORDS

Passwords

g. TRAIN YOUR STAFF TO BE CYBER AWARE

Make sure staff are trained to know the benefts of operating digitally, but are also aware of cyber security threats and how to deal with them. Due to the rapid development and changes in digital technology it is a good idea to add cyber security to your annual training plans/ matrix.

NHS Digital's Data Security Awareness Programme, in conjunction with Health Education England, includes Data Security Awareness Training

5. RESOURCE LIBRARY

The information below lists some of the organisations who offer advice to the public and businesses, including those in health and social care, about the best ways to protect devices and data.

Taking these actions will also be valuable with regards to the Department of Health guidance, Data Security and Protection for Health and Care Organisations, which outlines the steps expected from health and care organisations up to and beyond April 2018.

NHS Digital

NHS Digital is where you will fnd information about The Data Security and Protection Toolkit which will be replacing the existing Information Governance Toolkit in April 2018.

Good Practice Guides are also available as well as information about national systems for health and care, such as NHSmail.

NHS Digital also has a Data Security Centre which has live reporting on cym1curity