NHS
Digital

1 Trevelyan Square
Boar Lane
Leeds LS1 6AE

0300 303 5678

14 May 2017

Dear colleagues

We are continuing to work around the clock to support NHS organisations that have reported any issues due to Friday's cyber-attack. This includes understanding the impact to both the acute sector and primary care.

How to reduce the risk of this type of attack:

- Make sure your security software patches are up-to-date
- Make sure that you are running up-to-date anti-virus software
- Back-up your data in multiple locations, including offline
- Avoid opening unknown email attachments or clicking on links in spam emails
- To understand more about ransomware and how to protect your organisation, please look at the best practice guides on the CareCERT Information Sharing Portal: https://nww.carecertisp.digital.nhs.uk/display/CC/Ransomware+-+Preparing+for+an+Outbreak
- Existing National Cyber Security Centre guidance provides organisations with information about how to protect themselves from ransomware attacks.

Patches to remove the vulnerability:

Patches to remove the vulnerability that 'WannaDecrypt0r' ransomware has exploited can be found here: **https://technet.microsoft.com/en-us/library/security/ms17-010.aspx**

- Infected computers should been disconnected from the network **immediately**, and before applying any patches. The machine should be restored and built from a known good back-up before being entered back on to a clean network or any centralised deployment methods are utilised.
- Patches can be deployed centrally by using systems such as WSUS, System Center Configuration Manager or third party update management solutions such as Zenworks.
- It's important to understand if the machines on your network have been patched, **if you're unsure please contact your local IT provider.**

How NHS Digital can help you with data security:

NHS Digital delivers a range of data security services that support NHS organisations to take appropriate cyber security measures and help them to respond effectively and safely to cyber security threats. These include:

- broadcasting information to NHS organisations about known cyber security threats and appropriate steps to take to minimise these risks, as was the case with this incident.
- protective real-time monitoring of national NHS IT services and systems, which have all been designed to have strong security measures.
- Undertaking free cyber security testing for NHS organisations and give them bespoke advice about appropriate steps they can take.
- training for health and care staff designed to ensure frontline workers are aware of their own responsibility towards ensuring cyber security in their organisations, and that they know the simple steps that they can take to help to keep their organisation secure.

To receive NHS Digital’s high-severity security threat alerts and advisories on data security please email carecert@nhsdigital.nhs.uk

The National Crime Agency (NCA) encourages anyone who thinks they may have been subject to online fraud to contact Action Fraud at www.actionfraud.police.uk. It is a matter for the victim whether to pay the ransom, but NHS Digital and the NCA encourages industry and the public not to pay.

Kind regards

Dan Taylor
Head of Security
Data Security Centre
NHS Digital