From the Permanent Secretary
Sir Chris Wormald

Department of Health & Social Care

39 Victoria Street
London
SW1H 0EU
permanent.secretary@dhsc.gov.uk

Rt Hon Meg Hillier MP
Chair of Public Accounts Committee
House of Commons
London
SW1A 9NA

Sent via email to: pubaccom@parliament.uk

3 September 2020

Dear Chair

Update on Public Accounts Committee recommendation following WannaCry

The Public Accounts Committee (PAC) report into the WannaCry cyber-attack on the NHS was published on 18 April 2018: Cyber-attack on the NHS – Session 2017-19 (HC 787).

There were six recommendations in this report. Five recommendations had previously been implemented (as per treasury minute Cm 9643). One recommendation as set out below remained a work in progress:

PAC conclusion: Not all local bodies have the means to update and protect systems without disrupting the ongoing delivery of patient care.

PAC recommendation: The Department and its arm's-length bodies should:

- *set out how local systems can be updated whilst minimising disruption to services, and provide guidance and support to do this;*
- *ensure that all IT suppliers and suppliers of medical equipment to the NHS are accredited and that local and national contracts include standard terms to maintain and protect NHS devices and systems from cyber-attack;*
- *and ensure that local and national workforce plans include a focus on IT and cyber skills.*

This letter provides detail on the measures implemented to complete the outstanding recommendation. We will also continue to improve these as part of our ongoing cyber security programme. We now consider this final recommendation closed.

Guidance and support for updating local systems

NHS Digital (NHSD) has now aligned its advice and guidance on updating local systems with that of the National Cyber Security Centre (NCSC), including guidance on implementing the EU Directive on the security of Network and Information Systems.

NHSD also provides regular advice and guidance to the NHS, through a weekly bulletin, setting out the risks associated with newly identified cyber vulnerabilities and details of appropriate actions organisations need to take to mitigate the cyber risk from each vulnerability. This is supplemented further by a High Severity Alert process, which is triggered when vulnerabilities are deemed serious enough to warrant assurance that all large NHS organisations have received and acted upon the advice from NHSD.

As part of a co-ordinated response plan to support the NHS and increase resilience during COVID-19, NHSD has worked with NHSX and the NCSC to provide a dedicated Technical Remediation service, providing NHS Trusts with identification and remediation of critical vulnerabilities. Furthermore, NHSD and the NCSC have undertaken proactive scanning for vulnerabilities on Internet-facing services for Trusts, identifying vulnerabilities that should be addressed in order to further improve local resilience. Where needed, NHSD have supported organisations to implement the required remediation to address these vulnerabilities.

NHS Trusts now benefit from access to Microsoft Defender Advanced Threat Protection (ATP), which provides real time detection and protection against potential threats by identifying suspicious behaviour on devices indicative of a cyber-attack. Rollout of Windows 10 is underway and as of July 2020, 68% of the NHS desktop estate successfully migrated to Windows 10. The NHS has been supported in this endeavour with guidance and support from NHSD to minimise disruption to services.

Supplier accreditation and standard contracts

The Data Security and Protection Toolkit (DSPT) requires local organisations to ensure that information technology system providers have appropriate accreditation. The DSPT includes the following mandatory requirement (ref 10.2.1. applicable to all types of health and care provider):

Organisations ensure that any supplier of IT systems that could impact on the delivery of care, or process personal identifiable data, has the appropriate certification.

In addition, Trusts and CCGs must also meet the following mandatory requirement (10.2.2):

Organisations should, as part of their risk assessment, determine whether the supplier certification is sufficient assurance.

NHSX has worked on the development of procurement frameworks, including the GP IT Operating Model and the Health Systems Support Framework, to ensure that cyber security is considered when selecting suppliers. NHSX will continue to review cyber security requirements in national contracts and procurement frameworks, working with NHSD to issue guidance for local contracts. NHSD supported NHS Shared Business Services to establish a Cyber Security Framework for the NHS, providing NHS organisations with an assured pool of suppliers from which to draw down local support and resources.

With regards to connected medical devices, NHSD has worked closely with the NCSC in publishing guidance to assist organisations in protecting medical devices. NHSD has also undertaken a survey of Health and Care organisations on securing connected medical devices (CMDs), along with targeted engagement with sample organisations. This work informs future initiatives to improve the security of CMDs and the cyber security approach in the future regulation of CMDs as these develop.

.

Workforce planning for cyber security

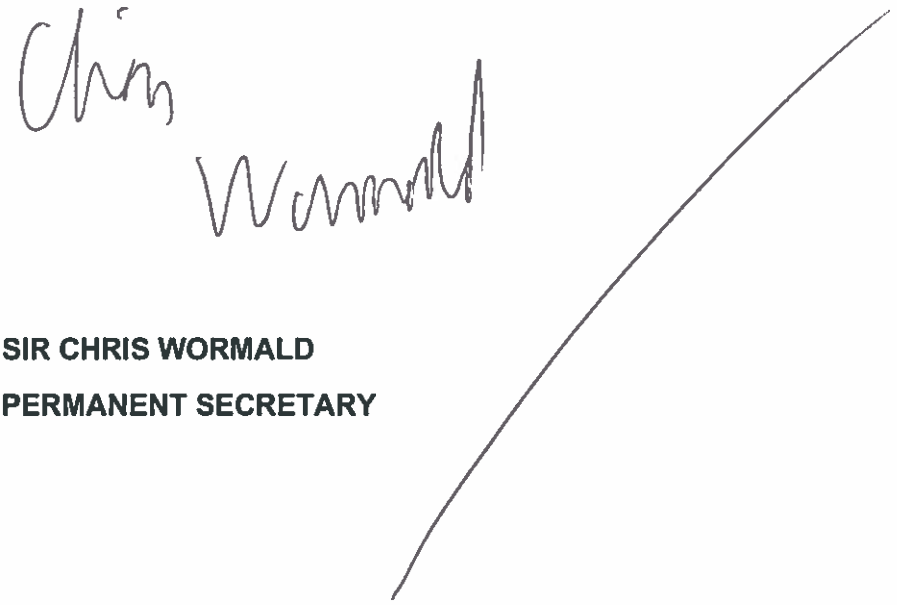
The NHS Long Term Plan sets out the importance of enabling a capable, digitally literate workforce to ensure security of NHS systems and data and to drive digital advances. Regional plans are being developed for recruitment of shared technical cyber resources across STP and ICS areas.

Board level leadership for cyber security also continues to be an area of focus. GCHQ-certified cyber security training has been delivered to 80% of Trust Boards (with a further 10% booked in to receive future training) and a specialist training course for Senior Information Risk Owner (SIROs) has been delivered to over 70% of Trusts.

Sharing data is critical to good patient care but data must be shared safely with all staff having a role to play. NHS staff are expected to complete the data and cyber security e-learning, developed in 2018 by NHS Digital and Health Education England (HEE). They must complete it annually with compliance monitored through the DSPT. NHS Digital continues to run its staff awareness campaign, Keep I.T. Confidential, to educate all NHS staff on steps they can personally take to reduce the risks of cyber incidents.

I hope the committee finds this update useful.

Yours sincerely,



SIR CHRIS WORMALD

PERMANENT SECRETARY