



To: Chief Executives of NHS Wales organisations

Cc: Andrew Goodall, Glyn Jones WG CDO, WG Data Protection Officer,
NHS Wales Chief Clinical Information Officers (CCIO)
NHS Wales Associate Directors for Informatics (ADIs)
COVID-19 Digital Cell Members
NHS Wales SIROs

29 October 2020

Annwyl Gyfeillion,

Cyber Security of NHS Wales Digital Systems

The digital response to Covid-19 has been exceptional and I am grateful to teams in your organisations for the work they are doing, individually and collectively. The accelerated adoption of digital technologies has created new opportunities but also potentially new vulnerabilities which could be exploited. It is essential that we maintain robust safeguards and processes, to protect our digital systems, and to respond effectively to cyber incidents.

National Cyber Security Centre

Cyber resilience and security are issues that affect all organisations and systems, and are a regular agenda item at the Covid-19 Digital Cell. I wrote to you in June to request that your organisation work with the National Cyber Security Centre (NCSC) and NWIS to provide assurance across NHS Wales. In England this was achieved through a direction from the Secretary of State to all NHS organisations, but the view of the Digital Cell was that Ministerial direction should not be necessary in Wales. I understand that all organisations have worked with NCSC and NWIS. For added assurance in this important area, please confirm that your organisation is now in contact with the NCSC, and is signed up to the NCSC Cyber Security Information Sharing Partnership. Further information can be found at <https://www.ncsc.gov.uk/section/keep-up-to-date/cisp>.

You may be aware of an increase in cyberattacks on public bodies in recent weeks - for example an incident at Hackney Council received widespread media coverage.

Rydym yn croesawu derbyn gohebiaeth yn Gymraeg. Byddwn yn ateb gohebiaeth a dderbynnir yn Gymraeg yn Gymraeg ac ni fydd gohebu yn Gymraeg yn arwain at oedi.

We welcome receiving correspondence in Welsh. Any correspondence received in Welsh will be answered in Welsh and corresponding in Welsh will not lead to a delay in responding.

It is important that all organisations regularly revisit their incident response plans and update them as appropriate. If a cyber incident is detected, there is a standard NCSC incident reporting process - all organisations must promptly report the incident to the NCSC and inform Welsh Government, collect and share all relevant information, and involve information governance leads if there is any possibility of a data breach or loss of data.

Network and Information Security Regulations

The resilience of some of our systems and services can be a case of life and death for the patients who rely on them, and these essential services are covered by additional *Network and Information Security (NIS) regulations*. Introduced in 2018, the NIS regulations form part of an EU directive setting out a framework for Operators of Essential Services (OES) in areas such as transport, water and health services to respond to cyber incidents which affect their operation. Work is underway by UK Government to transpose those regulations into UK law ahead of the end of the transition period.

Although cyber security is not a devolved matter, Welsh Government is the competent authority for the NIS regulations in the case of essential health services in Wales. Welsh Government is responsible for establishing the compliance framework for operators of essential services, which includes defining the scope of the regulations, reporting thresholds, and processes for reporting and dealing with cyber incidents. Although not all parts of NHS Wales will fall within scope of the NIS regulations, the security of our network and information systems is of relevance to us all. A networked system is only as secure as its weakest point. The compliance framework to be developed will therefore be transferable to other settings, to ensure a coherent approach to the reporting and management of cyber incidents across all organisations.

Welsh Government is working with a dedicated team in NWIS, which will in due course be hosted as part of the new Digital Special Health Authority. This Cyber Security Unit team will report into the new Digital Governance Framework and will have protected governance arrangements within the new organisation, in a similar approach to other regulatory functions such as GDPR compliance. Welsh Government will also continue to engage with NCSC and UK Government Departments to support this work.

A specialist cyber security consultancy firm with experience in establishing NIS regulatory frameworks in other settings has been engaged to support the development of the compliance framework and governance arrangements. They will start work in November and it is important that all organisations engage with this process, especially those identified as Operators of Essential Services under the NIS regulations. Please reply to this letter if for any reason you are unable to accept this request, on an organisational basis or for specific services.

Cyber Security and Freedom of Information requests

At the last Digital Cell we noted that a number of Health Boards and Trusts had received an FOI request relating to information on cyber security systems, and we

considered how to ensure consistency in responding to such FOI requests. For example, organisations may wish to develop written advice on the key considerations relating to digital systems and cyber security, which would be used to guide decisions on individual requests.

I have written to Covid-19 Digital Cell members, ADIs and CIOs asking that when organisations receive FOI requests relating to their IT systems or software they should seek the views of other organisations, NWIS, ourselves in Welsh Government, and others who may be affected by the disclosure of such information, before responding. This will allow us to better understand and consider the potential harms that may be caused by disclosing this potentially sensitive information.

I have also asked that if organisations have guidance in place already, or have recorded their rationale for consideration of individual requests of this type, it would be helpful to share that information, as a first step towards adopting common principles and guidance across all NHS Wales organisations.

Yn Gywir

Ifan Evans

Director –Technology, Digital & Transformation
Cyfarwyddwr –Technoleg, Digidol a Thrawsnewid