



Feidhmeannacht na Seirbhíse Sláinte  
Health Service Executive

## Minutes of HSE Board Meeting

Friday 21<sup>st</sup> May 2021

A meeting of the Board of the Health Service Executive was held on Friday 21<sup>st</sup> May 2021 at 16:00 by video conference.

Present: Ciarán Devane (Chairperson), Deirdre Madden (Deputy Chairperson), Aogán Ó Fearghaíl, Brendan Lenihan, Fergus Finlay, Fiona Ross, Yvonne Traynor, Tim Hynes, Sarah McLoughlin, Brendan Whelan, Anne Carrigy.

Apologies: Fergus O’Kelly.

In Attendance for Board Meeting:

Paul Reid (CEO), Colm Henry (CCO), Mark Brennock (ND Communications), Fran Thompson (CIO), Niamh O’Beirne (National Lead Test and Trace), Anne O’Connor (COO), Dean Sullivan (CSO), John Kelly (Corporate Affairs), Dara Purcell (Secretary), Niamh Drew, Amy Phillips, Hannah Barnes.

### **1. Update on the HSE Cyber Security Incident**

The Chair welcomed members to the meeting. No conflicts of interest were declared. The Chair outlined that the purpose of the meeting was for the CEO to brief Board Members on the HSE Cyber Security attack.

The CEO firstly took the opportunity to thank the Board for their patience in receiving an update on the cyber security incident and acknowledged the support, knowledge and contributions provided by Board member Tim Hynes over the period. The CEO expressed thanks to Tim for arranging the provision of temporary facilities to house the IT recovery room, and also to the senior AIB staff who brought their expertise in cyber, general IT, and incident management, and to the building and coordination of a group of experts who gave their time for free to support the HSE. He noted the intention to relocate the team to a HSE facility over the course of the weekend. The CEO acknowledged that the support given was a key enabler in the mobilisation and acceleration of the HSE response to this attack.

The CEO informed the Board that the HSE became aware of the attack in the early hours of the 14 May when an on-call critical incident co-ordinator escalated the matter based on several instances of

malware being identified noting that the Office of the Government CIO (OGCIO), National Security Centre (NCSC) and Gardai were informed within hours of the incident having been identified.

A cyber security incident response team (CSIRT) was immediately established under the leadership of the CIO and this team supported by a broad range of experts from across the technology, consulting, and the legal community. Clear roles and responsibilities have been established which have better enabled internal coordination and fostered a unity of effort and approach. The NCSC advised that the HSE should seek immediate specialist security support from a leading technology consulting firm, which is a leading global specialist in cyberattack detection, prevention and recovery. The CEO confirmed that the HSE has engaged with them.

The CEO proceeded to set out and provided insight on the four phases of the HSE's four stage critical incident response that is currently underway

(a) The Contain Phase – This is now complete

(b) The Inform Phase – This is also complete

(c) The Assess Phase – There are two integrated parts to this phase, currently in progress

and they are as follows:

(i) Operating System Level Assessment

(ii) The "Path to Green," which is the steps that need to be taken before any application can be restored

(d) Remedy – This phase is also currently in progress.

The CEO also provided an update in relation to the risk of unauthorised publication of patient data and informed the Board that the HSE's Data Protection Officer is providing support in relation to this. He informed the Board a High Court injunction had been sought and was secured, which has the effect of restraining any sharing, processing, selling or publishing of data stolen from the HSE's ICT systems.

The CEO also confirmed that a decryption key to unlock the data has been provided and work is now ongoing to assess the key and its potential to support restoration the HSE's networks and data noting the risks associated with this

The Board held a discussion with the EMT on the significant concerns regarding the risk the criminal ransomware attack poses to patient safety and the impact it has on health services, noting there will continue to be major disruptions.

The CCO advised this incident has impaired access to patient records, information management systems and timely accurate diagnostic tests, and as such, it creates a risk to patients as a result of inadvertent clinical error, delayed diagnosis and delayed treatment. The Board were informed slow but steady progress is being made in assessing the impact, and in initiating the process of restoring core IT systems. The COO and the CCO have also established an integrated clinical and operational risk subgroup of the National Crisis Management Team which will address the patient safety impact of the cyber-attack. The priority for integrated operations is to bring back key patient care systems in line with clinical priorities and to keep patients safe while maintaining essential care and support services. Work will continue to assess risk on an ongoing basis, this has meant putting in place new arrangements to maintain care and patient safety in hospital and community services. In response to questions from the Board on the prioritisation of services, the COO advised hospitals and community services are working closely with the CSIRT to get priority systems back online including radiology, diagnostic services, maternity and infant care, patient administration systems, chemotherapy and radiation oncology.

The Board also raised the importance of areas such as procurement and governance with the CEO and it was acknowledged the importance of robust procurement processes and strong financial oversight as significant costs will be incurred in this programme. The Board highlighted the opportunity to document the learnings of this process with the CEO and agreed to support the EMT to lead and scope out appropriate terms of reference in relation to this.

Discussions were held on the impact of the criminal ransomware attack on estimated recovery timelines, engagement with private hospitals, recruitment challenges and the impact in areas such as the Covid 19 Vaccine Programme and Test and Trace. The CIO assured the Board the mass vaccination programme is continuing and has been largely unaffected by the current difficulties. The ICT infrastructure supporting vaccination is cloud-based and there has not been contaminated, nor has there been any requirement to shut down this system. Following further questions on the Test and Trace system, the National Lead for Testing and Tracing advised COVID-19 test and trace services are functioning; but testing centres are operating as walk-in sites for those with symptoms rather than by referral, as the GP referral system, which interfaces with the HSE's ICT systems has been impacted. She assured these services have seen the usual levels of attendance over recent days.

Board member, Tim Hynes who has provided significant support to the CEO, CIO, NCMT and CSIRT informed the Board that contact had made contact with and received from a number of established strategic ICT partners, and noted that these firms are providing expertise across technology (including applications and data), cybersecurity, incident response, digital forensics, and legal and regulatory. He highlighted to the Board that there is no one strategy for addressing this attack and the challenges are significant.

He advised that although there is significant importance to scope out the learnings from this attack, it must not interfere with recovery which must remain paramount for now. The Board conveyed their appreciation to the EMT, NCMT and CSIRT for their pragmatic response and to all the healthcare staff who are continuing to work through such unprecedented challenges. The Board acknowledged and thanked Board member Tim Hynes for his robust contribution to the response of the ransomware attack.


The Board condemned the criminal ransomware attack.

## **2. AOB**

The Chairperson thanked all in attendance for their contributions and discussions. He informed the Board next week's Board meeting will be slightly shorter as a number of agenda items cannot take place due to the cyber security incident.

He also briefed the Board on advice received from NIAC in relation to the vaccination of the 40-49 age-group cohort and it was agreed the correspondence will be circulated to the Board when systems are back up and running .

The meeting concluded at 17.35pm.

Signed 

**Ciarán Devane**

**Chairperson**

**Date: 25.06.21**