



Feidhmeannas Seirbhíse Sláinte
Health Service Executive

Office of the Chief Information Officer
delivering eHealth Ireland,
Dr. Steevens' Hospital
Steevens' Lane
Dublin 8

Ph: 01 635 2732
Fax: 01 635 2740

12th November 2021

Mr. Cormac Devlin TD
Dáil Eireann
Leinster House
Dublin 2

Re: PQ ref 52163/21

"To ask the Minister for Health the progress of the restoration of services and systems following the cyber-attack earlier in 2021; and if he will make a statement on the matter."

Dear Deputy Devlin,

1. Background

- 1.1 The cyber-attack was logged with the Office of the CIO on 14th May 2021. The HSE convened the National Crisis Management Team to co-ordinate and manage the HSE response to the attack through a Cyber Security Incident Response Team. The HSE informed the relevant authorities including the Data Protection Commissioner, an Garda Síochána and the National Cyber Security Centre. In addition, the Defence forces were also informed.
- 1.2 The CEO convened and chaired the National Crisis Management team who oversaw and managed the HSE response to the Cyber Attack.
- 1.3 The HSE engaged several partner organisations, Mandiant Fireeye a global specialist in cyber recovery and defence and a number of the professional services firms. Legal advisers who specialise in cyber-attacks were also engaged. The HSE recovery team included regional and national employees from the operational service, clinical and ICT. The focus was the safe delivery of patient care. The cyber security response contained four stages/phases and the current status is set out below:-
 - i. The **Contain Phase** – Contain the spread of the ransomware and its impacts
Status: complete

- ii. The **Inform Phase** – Ensure that all stakeholders internal and external are fully informed on the impacts and the recovery efforts
Status: complete - a weekly update is provided all the operations acute group CEO's and CHO's leads
- iii. The **Assess phase** – Restoration of services and eradication of ransomware and potential bad actors from the HSE and voluntary network,
Status: 99% complete
- iv. The **Remedy Phase** – Strengthening our network against future cyber treats, increasing the cyber profile of the HSE and applying the lessons from the present attack
Status: Ongoing the Mandiant recommendations are being implemented and the HSE has deployed 3 security operations centres, Microsoft for our 365 tenant, Caveo for our Anti-Virus Defence and Mandiant Cyber Security Defence.

2. Current Status

2.1 The prioritisation of systems to be restored was agreed in conjunction with the Chief Operations Officer and the Chief Clinical Officer. The approach to prioritisation was on a hierarchy of clinical and operational risk and to reflect the requirements of the service and is outlined in the table below, across Community, Acute and Business/Corporate services and national enablers:-

Approved Priorities Enablers	
Community	Community
1 Older Persons: Nursing Home Support Scheme 2 Older Persons: Residential Care 3 Older Persons: Clinical Notes 4 Older Persons: Home Support Services 5 Older Persons: Assessment 6 Cross Functional: Remote Consultations 7 Cross Functional: Webex 8 Cross Functional: Shared Folder Access 9 Cross Functional: Blueye 10 Cross Functional: Health Atlas 11 Cross Functional: Rostering 12 Primary Care: Orthodontic 13 Primary Care: Audiology 14 Primary Care: Dental 15 Primary Care: Civil Registration 16 Primary Care: Ophthalmology 17 Primary Care: Podiatry Services 18 Primary Care: Occupational Therapy Services 19 Primary Care: Community Pharmacy 20 Primary Care: Regional Immunisation Systems 21 Primary Care: Physiotherapy Services 22 Primary Care: Child Health 23 Primary Care: Asdtra GP Out of Hours 24 Primary Care: Social Inclusion (Addiction Services) 25 Primary Care: National Counselling 26 Disability: Children Disability Services 27 Disability: Assessment of Need 28 Disability: School Leavers 29 Disability: National Ability Support System 30 Disability: National Day Services 31 Disability: (DSAMT) 32 Population Health: Public Health/Public Analyst Labs 33 Public Health: CIDR 34 Population Health: Screening Services 35 Mental Health: Patient Management System	36 Mental Health: CAMHS 37 Mental Health: Appointment Scheduling 38 Mental Health: Cash Management and Registrar 39 Mental Health: Medication Management 40 Mental Health: Mental Health Tribunals 41 Environmental Health 42 Child Protection Service 43 Health & Wellbeing: Sexual Health Prevention & Promotion 44 Cross Functional: Digital Dictation 45 Primary Care: Newborn Bloodspot Screening 46 Primary Care: Schemes Administration 47 Primary Care: Aids & Appliances 48 Primary Care: Palliative Care 49 Primary Care: Chronic Disease Management 50 Primary Care: Therapy Services, Public Health Nursing & CIT 51 Primary Care: Practice Management Systems 52 Primary Care: GP Referral Systems 53 Disability: Acquired Brain Injury 54 Health & Wellbeing: Smoking Cessation (Quitmanager)
	Acute
	1 Patient Management Services (incl. ED and ICM) 2 Diagnostic Imaging 3 Laboratories 4 Radiotherapy 5 Maternity / Newborn 6 Endoscopy 7 Medical Oncology 8 Renal 9 ICU 10 Decontamination (CSSD) 11 Cardiology 12 Other Maternity systems: Evolution, Euroking, Viewpoint 13 Stroke (telemedicine) 14 Colposcopy 15 Audit: INOR 16 Critical Care: ICU Audit 17 Critical Care: Bed Information System (BIS)
	Business
	1 Payroll 2 Finance - Accounts Payable 3 Finance - General Ledger 4 Finance - Income 5 HR - Recruitment 6 HR - Training 7 HR Workforce Management 8 Reporting 9 HR - Document Management 10 Procurement 11 Supporting Services 12 Filemaker 13 Service Provision Governance
	National
	1 Primary Care & Reimbursement Service(PCRS) 2 EHC Card
#	Foundations / IT Enablers:
1	Infrastructure: networks, devices, etc HealthIrl, Citrix, Dameware, Remote Access
2	Email
3	Integration: Healthlink
4	Identifiers: IHI (Individual Health Identifier) Covid-ID

2.2 All of the priority systems have been restored and are functional.

2.3 In any cyber-attack, based on international learning, there is always a long tail of individual items that remain to be resolved. The HSE is working through these in a systematic manner however good progress has been made in resolving these.

- 2.4** Remote access for or staff and vendors is fully restored with the addition of additional cyber security measures to enhance the protection of our systems.
- 2.5** Email services are fully available in areas which had Microsoft Outlook, the two areas which used Lotus Notes are migrating to Microsoft Office. Email system are now fully functional for outlook users and are now treated as 'business as usual'. Lotus notes users are over 97% successfully migrated to outlook. The Remote Hubs commenced in the following Hospitals Louth, Monaghan, Navan, Cavan, Sligo, Letterkenny. Hubs continued until 22nd October to finalise the migration. Lotus notes migration has moved to a 'business as usual' mode of operation. In addition, the Lotus Notes archive mail is now available for all users. Microsoft Office archives are being restored on a user request basis. The HSE ICT Service Desk is available to manage any issues that may arise with emails on an ongoing basis.
- 2.6** The maternity system in the North-East was one of the systems which was problematic during the restoration. The system is now technically available and work is ongoing with the user community to test, validate and deploy it.
- 2.7** Healthlink services are fully technically available, the service has processed over 7.5 million messages since restoration of services in early June. The services in Healthlink include:-
- i. GP Messaging (PCRS reimbursement, GP Vaccinations, GP General Referrals, Covid Testing, Lap Orders, Chronic Disease Management, GP Vaccine Referrals and Social Welfare Sick Certificates)
 - ii. Individual Health Identifier Service
 - iii. Pharmacy Vaccinations
 - iv. Discharge Summary Notifications

I would also like to acknowledge the enormous efforts that HSE staff from every part of the organisation played during the cyber-attack, in order to continue to deliver health service while recovering our ICT systems.

If you feel that the question has not been fully answered or you require any further clarity, please contact me.

Yours sincerely,



Fran Thompson,
Interim Chief Information Officer, OoCIO, HSE.