An Stiúrthóireacht um Ardchaighdeáin agus Sábháilteacht Othar
Oifig an Phríomhoifigigh Cliniciúil

National Quality and Patient Safety Directorate
Office of the Chief Clinical Officer

A mixed methods analysis of the effectiveness of the patient safety risk mitigation strategies following a Healthcare ICT failure

Study Team

Dr. Michael Carton, Grainne Cosgrove, Fiona Culkin, Loretto Grogan, Catherine Hogan, Emma Hogan, Loretta Jenkins, Zuneera Khurshid, Margaret McGarry, Dr. Gemma Moore, Dr. Orla Healy

Commissioned by

Dr. Colm Henry

National Quality and Patient Safety Directorate

January 2022

Version [1]

Reader Information

Acknowledgments:	Dr. Michael Carton, Grainne Cosgrove, Fiona Culkin, Loretto Grogan, Catherine Hogan, Emma Hogan, Loretta Jenkins, Zuneera Khurshid, Margaret McGarry, Dr. Gemma Moore, Dr. Orla Healy
Developed by:	Health Service Executive National Quality & Patient Safety Directorate & Office of the Chief Clinical Officer
Title:	A mixed methods analysis of the effectiveness of the patient safety risk mitigation strategies following a Healthcare ICT failure
Version Number:	V1
Published Date:	10.01.2022
Subject:	This document presents a mixed methods analysis of the effectiveness of the patient safety risk mitigation strategies following a Healthcare ICT failure.
ISBN Number:	978-1-78602-191-5
Cite this document as:	HSE NQPSD (2022) A mixed methods analysis of the effectiveness of the patient safety risk mitigation strategies following a Healthcare ICT failure. Dublin: National Quality and Patient Safety Directorate (NQPSD) of the Chief Clinical Officers Office, Health Service Executive
For further information contact:	National Quality and Patient Safety Directorate E-mail: NQPS@hse.ie
Associated documents:	
Revision date:	
Access:	National Quality and Patient Safety Directorate website https://www.hse.ie/eng/about/who/nqpsd/qps-intelligence/qps-intelligence-reports

Creative Commons License and Legal Disclaimer

This publication was developed by the Health Service Executive (the "HSE") specifically for use in quality, patient safety and improvement initiatives. The HSE shall have no liability, whether in contract, tort or otherwise, for any injury, loss damage or claims whatsoever arising out of or in connection with, any third party's use of the materials or any part thereof. Please contact the National Quality and Patient Safety Directorate team by email at NQPS@hse.ie for more detailed information on the terms and conditions of use.

Acknowledgements

The study team wishes to express their sincere thanks to the participants of this study who generously gave their time to share insights and learning to inform the findings. We would also like to thank all HSE staff who assisted us in the participant recruitment process and facilitated us in setting-up the online focus group sessions. In addition, we are also thankful to all individuals who provided feedback on this report.

Executive Summary

Purpose:

The ‘Conti’ cyber-attack in May 2021 impacted the Information Communication and Technology (ICT) systems of the Irish health system, leading to a disruption in health and social care service delivery. The frequency and magnitude of cyber-attacks has risen sharply during the past few years and health systems are among the top targets of cyber-attacks. The purpose of this study was to understand the clinical impact of the Conti cyber-attack on patient safety, the mitigations staff put in place, and to capture the key learnings from front line staff affected by the attack.

Scope:

The HSE National Quality & Patient Safety Directorate commissioned a comprehensive, mixed-methods research study to meet this objective. The first step of the study was to conduct a literature review to inform the study design and to contextualise the learning. This was supplemented by an analysis of operational and clinical call logs of the cyber-attack response. This helped in identifying the services that were most impacted during the cyber-attack which included radiology, pathology/labs, radiotherapy, maternity, primary care, and disability services. The study was organised into three work packages.

Methodology:

Work package 1 was based on a quantitative content analysis of risk registers and an incident analysis. The content analysis of risk registers was analysed for the frequency of risk reporting across categories and business areas, word frequency and sentiment analysis. Incident analysis was conducted on all incidents reported throughout the health system during the period of the cyber-attack to identify those relevant to the cyber-attack. Work package 2 focused on quantitative analysis of routinely available national data using statistical techniques including descriptive statistics and Statistical Process Control (SPC) chart methodology. Work package 3 was based on a qualitative analysis of after-action review (AAR) documents conducted locally by the QPS teams within Operational Divisions, Community Health Organisations and Hospital Groups. Focus groups were conducted within a large hospital, a maternity hospital and a CHO area with healthcare teams impacted by loss of clinical systems. A thematic analysis of the AARs and focus groups was conducted.

Findings:

The study findings revealed that the impact of the cyber-attack was abrupt and widespread and healthcare teams lost access to most systems. The teams responded with resilience and adaptability to quickly develop manual workarounds to ensure continuity of services. However, these manual workarounds were prone to risks such as redundancy, missing data, and retrospective data entry and reconciliation. Even though there were no patient safety incidents reported during the study duration, staff were concerned that risks and incidents may emerge in future.

Work package 1 findings revealed that the most frequently reported categories of risk during the cyber-attack were lack of system access, patient harm, communication issues, lack of access to patient data, cessation of services, manual processing, and appointment scheduling. Work package 2 findings based on the analysis of the 16 routinely collected indicators revealed signals of dis-improvement in one indicator (percentage of all attendees aged 75 years and over at ED who were discharged or admitted within 6 hours). The number of delayed transfers of care was also above the upper control limits of the SPC during the duration of the cyber-attack. Work package 3 findings showed that healthcare staff in acute settings were more impacted than community care as they are more reliant on technology. There was a consensus that the contingency plans in place were not adequate for a downtime event that was system wide and long-lasting. Although there were major delays in service provision, the response of staff ensured patient safety and care was prioritised. The cyber-attack had a negative effect on staff who were already suffering from fatigue owing to the COVID experience. Communication was identified as a critical element in the success of the cyber-attack response. The cyber-attack also revealed the disparities in ICT infrastructure between acute and community healthcare areas.

Key Learnings and Conclusion:

The Conti cyber-attack on the Health Service Executive (HSE) in May 2021 had a significant impact on many HSE services. The findings of the study and literature support that the services with the highest levels of digitisation are most severely impacted by ICT downtime events. The metrics analysed showed that the impact on service users and families was less than that associated with the Covid-19 pandemic response and can be attributed to the significant efforts of staff to maintain services. No incidents directly attributed to the cyber-attack were identified in our analysis. The findings show that the impact of the cyber-attack on staff stress was significant. It is a key learning of this report that patient safety strategies are significantly strengthened through the use of ICT systems. Informing contingency planning for possible future ICT outages is therefore a key aim of this report and will help to ensure that patient safety remains central to the delivery of care.

Table of contents

1. Introduction

1.1 Background

The Institute of Medicine (IoM) defines patient safety as the prevention of harm to patients (1). Patient safety has evolved into an important discipline within the healthcare professions that applies safety science to achieve a trustworthy system of healthcare delivery (2). Patient safety is a priority for all healthcare delivery systems and its importance is reflected in the six domains of healthcare quality (3). In the Irish Healthcare system, the Patient Safety Strategy (4) commits to patients receiving the safest care possible ns outlines the priorities for improvement in patient safety. Several clinical and improvement programmes are positioned at national level to support learning and improvement in key areas including healthcare associated infections, sepsis, medication safety, and the prevention and treatment of deteriorating patients (4). At the frontline of healthcare delivery, patient safety is enabled by information and communications technology (ICT) applications such as diagnostic systems primarily laboratory and radiology systems, Electronic Health Records (EHRs), patient administration and pharmacy systems. This highlights the important role of cyber security in ensuring patient safety.

Amid a spate of international cyber-attacks, healthcare organisations have become among the top targets of attack by cyber criminals (5). Healthcare services are especially vulnerable to cyber-attacks due to the nature of services where any disruption can have a devastating impact on patient safety (6). Cyber-attacks on healthcare systems undermine the safety of patients as they often lead to loss of access to electronic health records, radiology, and pathology results. In worst case scenarios removing access to these key systems has the potential for patient harm (7). The risk of cyber-attacks on health systems has amplified during the COVID-19 pandemic due to increased remote work and reliance on virtual methods of care delivery. Cyber criminals have sought to exploit the vulnerabilities of the healthcare sector during this period (8, 9).

The future of health services will be shaped by increased digitisation which indicates an urgent need to understand the cyber security threats to patient safety, and to develop credible strategies to counter these unavoidable threats (10). While there is growing interest in research on cyber-attacks in healthcare the available literature is still limited (6). Despite its significant impact on patient safety, the healthcare sector lags behind other sectors in its ability to protect data from cyber-attacks (11). There is not only a gap in current research about the impact of cyber-attacks on patient safety but also an emerging need for research to improve health services' cyber security with the impending digital transformation of health systems in future. Downtimes due to cyber-attacks should be viewed by health systems as an opportunity to appraise the current systems and processes to ensure patient safety and enhance cyber security in the future. However, health systems are complex, and it is challenging to fully understand the impact of cyber-attacks on patient safety, highlighting the need for blended research approaches that investigate qualitative and quantitative aspects of the impact of cyber-attacks. Research suggests a need to recognise and integrate improvement in cyber security in health systems into the strategic improvement needs of the system (11). This represents an overlap between cyber security and improvements in quality and patient safety domains and highlights the need for further research in this space to mitigate the impact of cyber-attacks on patient safety.

1.2 Cyber-attack on the Irish health system

On Friday, 14th May 2021, the Health Service Executive (HSE) of Ireland was the target of a cyber-attack on its ICT systems. This Conti cyber-attack had a significant impact on many HSE services. As a first response, hospital, and health service IT systems were shut down to protect systems and patient data. While this represented a major risk to the integrity and privacy of medical and personal data, it also resulted in the disruption of services. In the initial few days after the cyber-attack, in the absence and/or limited availability of ICT systems, the health service focused on implementing manual work-arounds to ensure continuity of services. The HSE rapidly established integrated governance structures to oversee and expedite the clinical and operational response. Priority health services including patient administration systems, radiology, diagnostics, maternity, and oncology were prioritised in the work to resume systems.

The National Cyber Security Centre (NCSC) in collaboration with the HSE is taking the necessary measures to respond to the cyber security incident with work underway in ICT and operational divisions to rebuild the services. This report complements the review of the cyber-attack completed by PWC but specifically focuses on clinical impact and clinical learning. This study was commissioned by the Chief Clinical Officer and and led by the National Clinical Director for Quality and Patient safety, with the study team drawn from members of the National Quality and Patient Safety Directorate (NQPS) combining quantitative and qualitative skills. The NQPS Directorate of the HSE, located in the office of the Chief Clinical Officer is responsible for assessing and supporting improvements in the delivery high quality and safe services. The study team applied a mixed methods study to conduct a timely review of the mitigations and contingencies adopted in the Irish health system to minimise the impact on patient safety. In addition, the study focuses on the learning's regarding what worked well to inform future planning for further Information Communication Technology outages.

The purpose of this report is to present the objectives, literature review, methodology, findings, and key learning emerging from this study.

1.3 Research questions

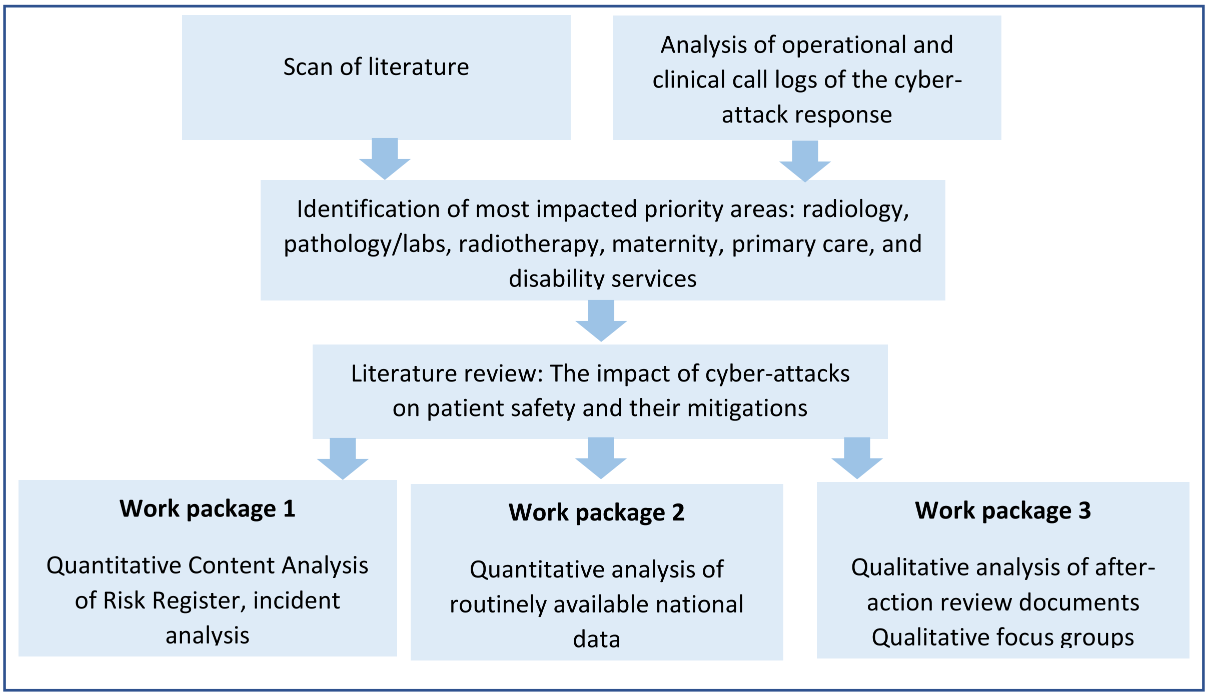
The objective of the study is to complete a comprehensive analysis of the clinical impact of the cyber-attack on patient safety; the mitigations put in place and the learning for the future. The central research questions of this study are:

- What are the risk mitigation measures and contingencies required to safely deliver patient services and maintain health and social care services in the event of an either partial or complete Information Communication Technology outage?
- What did we do, what worked well, where is there scope for improvement?

1.4 Research overview

The study utilised a blended approach based on multiple quantitative and qualitative data sources and consisted of three work packages. Work package 1 and 2 were quantitative while work package 3 was qualitative. Work package 1 comprised of a quantitative content analysis and incident analysis. Work package 2 involved quantitative analysis of routinely available national data. Work package 3 was qualitative and involved a thematic analysis of After-Action Review (AAR) documents and focus groups. An overview of the research process is presented in **Figure 1.1.** Details of each research step are provided in the methodology section.

Figure 1.1: Study overview



Scan of literature

Analysis of operational and clinical call logs of the cyber-attack response

Identification of most impacted priority areas: radiology, pathology/labs, radiotherapy, maternity, primary care, and disability services

Literature review: The impact of cyber-attacks on patient safety and their mitigations

Work package 1

Quantitative Content Analysis of Risk Register, incident analysis

Work package 2

Quantitative analysis of routinely available national data

Work package 3

Qualitative analysis of after-action review documents Qualitative focus groups

2. Literature Review

2.1 Introduction

A literature review was conducted both to inform the study design and to contextualise the learning for a wide audience. The impact on patient safety due to the loss of key systems, the mitigations put in place and the learning for the future was the focus of this review. Studies were retrieved from the peer-reviewed literature, using key search terms such as patient safety, risk mitigation and Information Communication Technology failure or outages. Eight databases were queried using the search terms included in **Table 2.1** (ProQuest, PubMed, Web of Science, Scopus, Embase, CINAHL, Wiley (Journal Package), Sage Health (Journal Package)).

Table 2.1: Details of Search Terms for Literature review

Band 1	Risk mitigation OR contingency planning OR emergency planning OR business continuity planning OR emergency preparedness OR risk avoidance
Band 2	ICT outage OR cyber-attack OR cyber terrorism OR ICT outage OR computer security OR system failure OR cyber security OR cyber threat OR critical downtime
Band 3	Patient services OR hospital patients OR care planning OR healthcare delivery OR EHR OR patient record OR electronic health record

The literature review was restricted to publications from 2016-2021. This is in recognition of the significant advances in Information Communication Technology in the last five years. The landscape prior to 2016 could be considered significantly different to the current reality. The grey literature was also in recognition of the significant temporal gap between such an occurrence and publication in the peer-reviewed literature. There is also a reasonable expectation that private healthcare systems may not wish to publicise being the victims of cyber-attacks, and some reports may only exist in the grey literature. Inclusion criteria focused on date of publication and the inclusion of empirical data on the patient safety impact of ICT technology failures. Simulation studies were included. Exclusion criteria were based mainly on publication date and the absence of empirical data. Several reviews, commentaries, letters, and editorials were excluded on the basis that no new empirical data was presented.

2.2 Summary of studies

Forty-nine papers were identified for review through the search strategy and two supplementary papers were added during the review process. Twenty papers were excluded based on review of the title and abstract and a further 21 papers were excluded based on full text review. The main reasons for exclusion included a focus other than patient safety impact (including how to prevent ICT downtime) and lack of original research (7 articles were opinion, letters to the editor or editorials, 6 articles were reviews with no original research included). A summary of the 10 papers that met the inclusion criteria are included in **Table 2.2**

Table 2.2: Summary of studies

Study (Country)	**Setting**	**Focus of Study**	**Methodology**
Coffey 2016 (USA)(12)	A National Institute of Health Clinical Centre	learning from a Specific EHR Downtime event (33 hours duration)	Qualitative Study: After Action Review
Dave 2020 (Australia)(13)	a large Australian 700-bed quaternary hospital providing acute medical, surgical, mental health, cancer, rehabilitation, and allied health services	Impact of an EHR Downtime Event (Caused by a cyber-attack) (6 days duration)	Qualitative Study: 9 interviews with staff
Scantlebury 2021 (United Kingdom)(14)	A large teaching hospital and neighbouring hospital (neighbouring hospital provided pathology services for both sites) The trust provides hospital services for 500,000 people and specialist services to 1.1 million people	Impact of a Pathology System Downtime Event (3 weeks duration)	Qualitative Study: semi structured interviews and focus group (sample limited to 16 key clinicians and hospital board members)
Wang 2016 (Australia)(15)	A 350-bed metropolitan teaching hospital	Impact of several Pathology System Downtime events (5 events over 11 months with duration ranging from 5 to 300 minutes)	Matched Case Control Study using 4 indicator laboratory tests (Potassium, Troponin, Haemoglobin and APTT)
Chen 2021 (USA)(16)	Tertiary referral hospital (radiology department)	Learning from a desktop simulation of a Radiology System Downtime Event based on experience of a ransom-ware attack	Desktop simulation of a cyber-attack
Larsen 2019 (Australia)(17)	300-bed suburban acute care facility with a 24-hour operating emergency department	Impact of downtime on pathology services	Hybrid Qualitative and Quantitative Study: comparison of downtime and normal activity data for 15 specific laboratory tests. Semi-structured interviews carried out (17 staff interviewed)
Magrabi 2016b (Australia) (18)	General Practice	Analysis of the impact on patient safety of different types of ICT errors	Qualitative analysis of incident reports: Prospective study with 87 GPs recruited to report incidents over a 19-month period
Ghafur 2019 (United Kingdom)(7)	NHS trusts across England and Wales	Impact of specific cyber-attack (the 'wannacry' attack) across all services in England and Wales.	Retrospective analysis of Hospital Episodes Statistics (HES)
Martin 2019 (United Kingdom)(19)	All NHS trusts across England and Wales	Impact and preventability of patient safety incidents due to ICT failures over a ten-year period	Retrospective analysis of incident reports over a ten-year period.
Larsen 2018 (USA)	Large Healthcare system in the mid-Atlantic region of the United States. The healthcare system includes urban, suburban, and rural hospitals	Categorising safety events associated with an EHR downtime period and evaluating adherence to downtime procedures	Retrospective analysis of Incident reports over a three-year period.

Three articles were related to specific ICT downtime events at individual hospital sites with predominantly qualitative methodologies employed to understand the impact on patient safety of technology failures. A further three articles examined the impact of ICT downtime at individual hospital or department level by looking at a series of events or by using simulation data. Of these six papers, three used pathology systems as the specific example, while two related to EHRs and one was related to a radiology system. The remaining four papers described an analysis of incidents or outcomes across a healthcare system. Three of these studies were retrospective with one prospective study included from general practice. A range of settings and methodologies were represented in the final synthesis. The following section presents some key points that were used to inform the study design and analysis of the current research.

2.3 Major themes

The impact on patient safety of healthcare technology failures was consistent, regardless of the cause of the failure. The literature referred to both planned and unplanned downtime events:

- Unplanned downtime events described in the literature included those caused by Cyber-attack, Power Outages, Flooding damage, Hardware failures and software failures. The duration of unplanned downtime events was unpredictable and varied widely between hours to weeks.
- Planned downtime events were associated with planned hardware or software upgrades or essential maintenance. Planned downtime events usually lasted a matter of hours.

Chen and co-authors have also published other useful research in this area including an analysis of the patterns and causes of digital downtime (20). The analysis of 128 events over a 33-month period showed that computer related network issues accounted for most downtime events (77%) with power outages and software related downtime also featuring prominently. The duration of the downtime events described in the included articles ranged from 33 hours (12) to three weeks (14). Although the impact of the cyber-attack on the HSE lasted many weeks, many of the themes that emerged from the review are still valid.

One article (16), based on a simulation exercise, described four phases of response for a downtime event that are useful for understanding the sequence of issues during prolonged downtime. Although written from the perspective of a radiology system, the construct is applicable to the wider context of healthcare ICT downtime. Generalising the points made in this article, the following is a useful guide for giving context to the findings of this report and the potential risks and mitigations associated with each phase:

Hyper-acute phase (first 48 hours): The focus was on ensuring patient safety, prioritisation based on clinical need, and assessing which systems are impacted and the scale of the impact.

Acute phase (days to weeks): Analog systems and workarounds are in routine use and good communication and clear roles are key mitigations of the risks associated with technology failure. It is possible during this phase that a combination of low technology (e.g. paper based systems) processes is running alongside partially restored high technology processes.

Infrastructure recovery: This is largely a non-clinical activity, but communication with clinical staff is important to ensure the benefits of system restoration are as expected. Depending on the scale of the technology failures, restoration of key systems and functionality may be on an incremental basis.

Reconciliation phase: Once systems are restored, data that exists in analog format only must be back loaded to the ICT systems to ensure continuity of clinical data for future clinical interactions.

Table 2.3 is included as a useful example of how to approach planning for significant downtime events. Although the example is based on a radiology system, the findings can be adapted for contingency planning for other healthcare systems. **Table 2.3** presents a readiness checklist for physician teams in radiology, reproduced from Chen et al (16)

Table 2.3: Cyber-attack readiness checklist

Phase 0 (plan now—readiness)

- Plan for communication for a sudden outage within the section and with critical services
- Phone number and emails for the section
- Location to store downtime manual binder
- Assign a safe, locked location for documents containing patient information such as written reports
- Engage enterprise collaborators on "special workflows"—for instance, stroke patients, intraoperative workflows, surgical foreign bodies
- Instructions for immediately needed processes like medication locker override
- Reference resources—such as book of protocols, textbooks (if needed)
- Alternative section schedule planning for at-modality interpretation
- Assess departmental interdependencies with other departments that you serve have a plan for communication with the departments

Phase 1— (First 48 h)

0–2 hours

- *Create protocol for immediate assessment to ensure the safety of current patients including diagnostic and procedural areas*
- *Identify a single downtime person to communicate with incident command*
- *Assess the extent of impact on workflow on diagnostic modalities*
- *Assess the extent of impact on workflow on diagnostic workstations*
- *Check phone lines and fax machines for functionality*
- *Identify the critical workflows that require additional attention. E.g., Acute stroke*
- *Trigger paper-based ordering and findings process for diagnostic examinations*
- *Trigger paper-based interventional procedure ordering and triage*
- *Prioritize immediate patient care demands. E.g. emergency, intensive care, urgent care, pre-operative, inpatient, outpatient*
- *Identify the examination types that require verbal findings communication for every case*

2–24 hours

- Review items established during 0–2 h
- Determine the priority of future and pending outpatient orders. Which exams/if any must be cancelled/postponed so all remaining services can be properly staffed by physicians?
- Reassign staff as needed—staff might need to work off modalities till air-gapped independent systems are in place

24–48 hours

- Review items established during 0–24 h
- Contact incident command for an updated status on operational impact
- Review plan for staffing changes and exam prioritization
- Identify imaging centres and locations no longer feasible for service, if any

Phase 2 (initial days to several weeks)

- Review phase 1 recovery plan
- Maintain contact with incident command for updated status and coordinate recovery of clinical operations
- Connect with IT for new digital assets such as clean offline computers
- Readjust physician task and shift modifications based on new workflow demands

Phase 3 (several weeks to months)

- Work with IT to have a backup copy on a separate network if possible and to plan for rebuilding infrastructure using clean assets

Phase 4 (several weeks to months)

- Paper-based workflow should have a systematic way to document patient and exam identifiers and record contrast and radiation dose (as needed)
- Transcribing the paper report to digital form would be needed to store this information in EMR
- Images stored on analog media should be correctly labelled to aid in eventual reconciliation with PACS and EMR

Two articles pointed out the difficulties in retrospectively entering missing data on affected systems. For example, the relationship between the length of downtime (33 hours) and the time required to update data on restored systems (approximately one week) as reported in one study is noteworthy (Coffey et al, 2016). The scale of effort required to backload data should therefore not be underestimated.

A common theme throughout the literature reviewed was the need for contingency planning for ICT downtime events. This can be considered part of emergency planning and significant resource is required to ensure that low technology or analog systems are prepared in advance and can be implemented quickly. Paper-based systems are described alongside good communication among all staff. Other low technology solutions such as fax and phone are also routinely described as part of contingency planning. Larsen et al., (2018) considered the issue of adherence to downtime procedures and showed that procedures were either not adhered to or not in place for 46% (n=35) of incidents reported.

In summary, the reviewed literature showed that the learning from research informs contingency planning for possible future similar events. There is evidence to suggest that the frequency of cyber-attacks on healthcare institutions in recent years has been increasing (21). It should therefore not be considered that future attacks are unlikely or that criminal activity considers healthcare anything other than a legitimate target.

Three papers included an analysis of incident reporting systems over a significant duration. These studies are therefore not associated with a specific downtime event. **Table 2.4** presents a summary of the types of incidents reported in these articles. The range of systems described where incidents were reported were consistent with those described in studies that capture learning from specific downtime events (Pathology, Radiology, and Pharmacy systems). The types of incidents were also consistent with those presented in this review (e.g. patient identification, ordering diagnostics, reporting findings, medication errors, and delays in treatments). Martin et al. (2019) also included the issue of failure of medical devices. This was a useful addition to the discussion on the possible reach of ICT technology failures.

Table 2.4. Types of incidents reported related to technology failures

Study	Larsen et al, 2018	Martin et al., 2019	Magrabi et al., 2016
Number of incidents related to ICT downtime or ICT failures (timeframe)	76 incidents (over 3 years)	2627 incidents (over 10 years)	90 incidents (over 19 months)
Top five most frequently reported types of incidents	Pathology related (Patient Identification incidents, Ordering of tests, Reporting Findings) Imaging (Ordering Diagnostics and Reporting Findings) Medication (Ordering medications, delays, wrong dose, wrong medication) Disrupted on incomplete Patient Registration Transfers and handover of patients at end of shift	ICT related Infrastructure (failure of systems or telecommunications, lack of skilled staff) Clinical assessment (delays in receiving findings, missing findings, incorrect findings, inadequate, missing or incomplete scans) Documentation (missing, inadequate, incorrect, delayed or no access to documentation) Failure, absence or unavailability of medical devices Medication related incidents	GP practice system failure Medication (wrong drug, wrong patient, incorrect dose, route or strength) Investigations (test findings and specialist letters reported for wrong patient) Communication Non-medication treatment incident

2.4 Impact of prolonged ICT downtime on patient safety

The types of impact on patient safety that finding from prolonged ICT downtime are varied. Some key aspects are listed here:

2.4.1 Accurate patient identification

The use of handwriting instead of printed stickers and barcodes was necessary for pathology testing and this introduced the possibility of transcription error or incorrect information being recorded.

2.4.2 Delayed treatment

Switching to analogue or paper systems slowed down processes. In one example, pathology departments asked clinical areas to reduce the amount of lab tests ordered to compensate for the increased workload on staff. Even in a scenario where individual analysers worked off-line; extra time was required for sample processing and findings reporting. One incident included in Martin et al. (2019) described a delay in gentamycin treatment due to inability to access gentamycin level findings in paediatrics. Wang et al (2016) also described delays in laboratory diagnostics in more detail. Other diagnostics such as radiology featured prominently in incidents reported and include issues with ordering, transfer of images for interpretation and transmission of findings to physicians.

2.4.3 Decision support

Medication safety is enabled by several factors including system prompts for prescribers. Incidents related to dosage and wrong medication have been reported as an impact of ICT system downtime. Decision support is a feature of many systems including Electronic Health Records, Pathology, Pharmacy and Radiology. Another example presented in the literature was the absence of reference ranges on pathology reports and its impact on treatment or delays to treatment.

2.5 Limitations of the review

A limitation of the review was that included studies were all based in high income countries only. Another limitation was the risk of publication bias as private healthcare organisations may not wish to publicise being the victims of cyber-attacks. Furthermore, no studies reviewed looked at events that were greater than three weeks.

2.6 Conclusion

In the context of patient safety, the cause of the ICT downtime event is irrelevant and contingency planning should be viewed as an integral part of implementing healthcare ICT systems. It is reasonable to suggest that the examples and themes listed here and in the literature are likely to be repeated in any ICT system downtime event in healthcare. Across all articles reviewed, the issues of accurate patient identification, delays in treatment, difficulties accessing diagnostic findings, decision support, missing or inaccessible clinical information and medication safety featured prominently. There were also many indirect impacts on patient safety. Issues such as delayed discharges / admissions, difficulties in hand-over, difficulty recording clinical information were all significant.

3 Methods

This study was based on a mixed methods approach encompassing quantitative and qualitative methods. The research was divided into three work packages, work packages 1 and 2 focused on analysing quantitative data collected prior to and during the cyber-attack. Work package 3 involved collecting and analysing qualitative data.

3.1. Work package 1

Work package 1 comprised of content analysis of risk registers and incident analysis.

3.1.1. Incident analysis

The Incident Management Framework defines an incident as *"an event or circumstance which could have or did lead to unintended and/or unnecessary harm*" (22). Incidents reported throughout the Health Service Executive during the period of the cyber-attack were analysed to identify the number of incidents, relevant to the cyber-attack and the impact of these incidents. The Incident Management Framework (2020) was used to guide this analysis (22). Within the Health Service Executive, services report an incident either by completion of the appropriate National Incident Report Form (NIRF) or a direct entry on the National Incident Management System (NIMS) if available. Reporting of an incident should be done as soon as is practicable after the incident occurs (22). Due to the cyber-attack, services were unable to access the NIMS and so unable to upload incident notifications electronically. A contingency process was implemented allowing all services to submit their existing hardcopy NIRFs to the State Claims Agency (SCA) for uploading onto NIMS.

Data for this analysis was extracted from the National Incident Management System (NIMS) on 23rd August 2021 as per the below criteria:

- Location at Level 1: 'Healthcare'
- Who/What variable = Incidents relating to patient and dangerous occurrences are included
- For graphs/tables showing Date of Incident; YTD numbers for 2019, 2020, and 2021 are used
- For graphs/tables showing Incident Report Date; year to date (YTDD numbers for 2019, 2020, 2021 are used

On receipt of NIRFS by the SCA, incidents were uploaded to NIMS by four business units within the SCA and a quality assurance (QA) process was undertaken by risk advisors as incidents were being uploaded. During QA, a sample of service user incidents (those checked by the Clinical Risk Unit) were further analysed to identify incidents directly related to the cyber-attack itself. Some incidents were also identified by a keyword search. This yielded a sample of 244 incidents. A theme was applied to these service user incidents based upon the information that was available in the summary of the incident.

3.1.2. Content analysis of risk register

Risk registers for operational and clinical meetings stood up in response to the cyber-attack from 16/05/2021 to 08/06/2021 were analysed for frequency of reporting of risks across categories and business areas in categorical data fields, and for word frequency and sentiment in free text fields. Descriptive analysis for categorical variables was undertaken (counts, percentages, cumulative percentages, and cross tabulations) and presented in Pareto charts, and tables. The data were cleaned to ensure that each level of categorical variable was unique. Frequency analysis was conducted on free text variables (word counts and correlation of word pair) and presented in word clouds and tree maps. Prior to analysis, data were cleaned to remove punctuation, symbols and stop words (i.e., commonly removed words such as “and”, “the”, “at”). Sentiment analysis was conducted on free text variables using the NRC Word-Emotion Lexicon (23). This is a list of words and their associations with eight emotions (anger, fear, anticipation, trust, surprise, sadness, joy, and disgust) and two sentiments (positive and negative) (24). Analysis was conducted in R (25) and Excel. Packages used in R include “tm”, “wordcloud”, and “ggplot2”. Limitations of this analysis include the self-reported nature of risks. Risk frequency and risk rating may be biased by more engaged representation in the recording of risks in different Business Areas/Care Groups or Categories. Better stewarded areas of risks may be overrepresented in comparison to areas with less prior engagement in identification and reporting of risks.

3.2. Work package 2

A statistical analysis was undertaken to determine the impact of the cyber-attack on activity within the Irish public healthcare system. A representative suite of indicators from the HSE Management Data Report (MDR) and other national data sources were selected to reflect overall activity and patient safety in areas most impacted. Baselines for relevant indicators were established from 2019 data. This reflected a standard level of activity prior to COVID-19 and the cyber-attack. COVID-19 baselines were also explored, using data from 2020. Activity data from May and June 2021 was compared to these baselines. Data was analysed using statistical techniques including descriptive statistics and statistical process control chart methodology where appropriate. This phase was based on aggregate national data and did not require direct participant involvement from the sites.

Data sources include:

- HSE Business Intelligence Unit (BIU)
- Health Pricing Office (HPO) - Hospital Inpatient Enquiry (HIPE)
- National Treatment Purchase Fund (NTPF)
- National Cancer Control Programme (NCCP)
- Any other HSE sources.

All data presented was aggregated with no personally identifiable information. Data was held and processed in line with the HSE data protection policy and relevant agreements with data providers. The indicators included in the study are:

- Number of new and return outpatient attendances
- Number of people waiting for a first appointment at a consultant-led Outpatient clinic
- Percentage of patients waiting <52 weeks for first access to OPD services
- Number of new emergency department (ED) attendances
- Percentage of all attendees aged 75 years and over at ED who are discharged or admitted within 6 hours
- Number of inpatient discharges
- Number of day cases (including dialysis)
- Inpatient & day case active waiting list
- Number of delayed transfers of care
- Number of new people waiting more than four weeks for access to an urgent colonoscopy
- Percentage of patients waiting <13 weeks following a referral for routine colonoscopy or OGD
- Number of patients who completed radical radiotherapy treatment (palliative care patients not included)
- Number of patients triaged as urgent presenting to symptomatic breast clinics
- Number of patients attending rapid access prostate clinics in the cancer centres
- Number of patients attending rapid access lung clinics in the cancer centres
- Percentage of child health & development assessments completed on time or before 12 months of age

3.3. Work package 3

3.3.1. After action review (AAR) documents

An After-Action Review (AAR) is a structured facilitated discussion following an event that identifies key learning to inform improvement efforts. In healthcare, the AAR is frequently used by multidisciplinary teams following an incident and is included as a means of investigating incidents in the HSE Incident Management Framework (22). This method of organisational learning from experience fits well in the context of the impact on clinical practice of Information and Communications Technology (ICT) system downtime and has been noted as a methodology in the recent literature (12). The AAR was chosen as a method of data collection for the current study as it is already in use within the healthcare system in Ireland and is well recognised as a robust methodology for organisational learning (26). The four questions used are as described in the HSE Incident Management Framework (22):

- What did we expect to happen?
- What actually happened?
- Why was there a difference?
- What have we learnt?

For each AAR, a facilitator worked with the group to reach a consensus on the ground rules. The discussion began with the background to the incident. A scribe supported the AAR by keeping anonymised notes based on the discussion of the four questions and the outcome of the AAR was recorded using the AAR summary Report as described in section 15 (p. 100) of the Incident Management Framework (22). Participants provided feedback on the summary report and any amendments necessary were made prior to the report being included for analysis. AARs were conducted separately in acute settings, community healthcare organisations and at a national level. Where the scope of AARs extended beyond impacts on patient safety, only relevant information was extracted from the summary reports for analysis. The analysis of AAR documents was conducted by three team members who identified the themes while focusing on the patient safety impact of the cyber-attack.

3.3.2. Study procedures for focus groups

This work package explored the experience of staff working in acute, maternity and community settings. Eight focus groups were conducted with 36 participants using an in-depth semi-structured approach to explore:

- The impact of the cyber-attack on the delivery of services and patient care
- What mitigations were successful or unsuccessful from a patient safety perspective?
- Key learning to minimise the impact on patient safety in the case of an IT outage in the future.

The study received ethical approval from the Clinical Research Ethics Committee of the Cork Teaching Hospitals (ECM 4 (s) 6/7/2021 & ECM 3 (oo) 10/08/2021) (see **Appendix File 1)**. Different settings included in the study were a large University Hospital, a Maternity Hospital, and various sites from one Community Healthcare Organisation (CHO). In consultation with the relevant Heads of Service for Quality Safety and Service Improvement, representatives from services in these sites most affected by the cyber-attack were invited to participate in focus groups to share their experiences and learning. This included radiology, pathology/labs, radiotherapy, maternity, primary care dental services, and health, and wellbeing, COVID testing, older person's care, and disability services. A detailed study information sheet was provided **(Appendix File 2)** to potential participants. The focus groups lasted approximately 60 minutes each. The topic guide and questions focused on:

- The impact on the quality and safety of patient care during the cyber-attack
- The risk mitigation measures, contingencies and workarounds teams developed and of these what worked well
- The key learning to prepare for possible future outages

The complete topic guide is presented in **Appendix File 3**. Focus groups were conducted virtually using online platforms (MS Teams and Cisco WebEx) depending on the preference of the participants due to Covid restrictions. **(Appendix Files 4a and 4b)**. Informed consent was sought, and participants were given the opportunity to ask questions and voice any concerns and asked to sign a consent form. Following good practice, all qualitative data collected was anonymised to ensure individual participants, hospitals or services cannot be identified. The data collected was qualitatively analysed using thematic analysis using a widely applied, 6-step thematic analysis framework (27). One research team member conducted the thematic analysis using NVivo software (28) while a second team member reviewed themes to ensure trustworthiness of the qualitative analysis.

4. Findings

4.1. Work package 1 findings

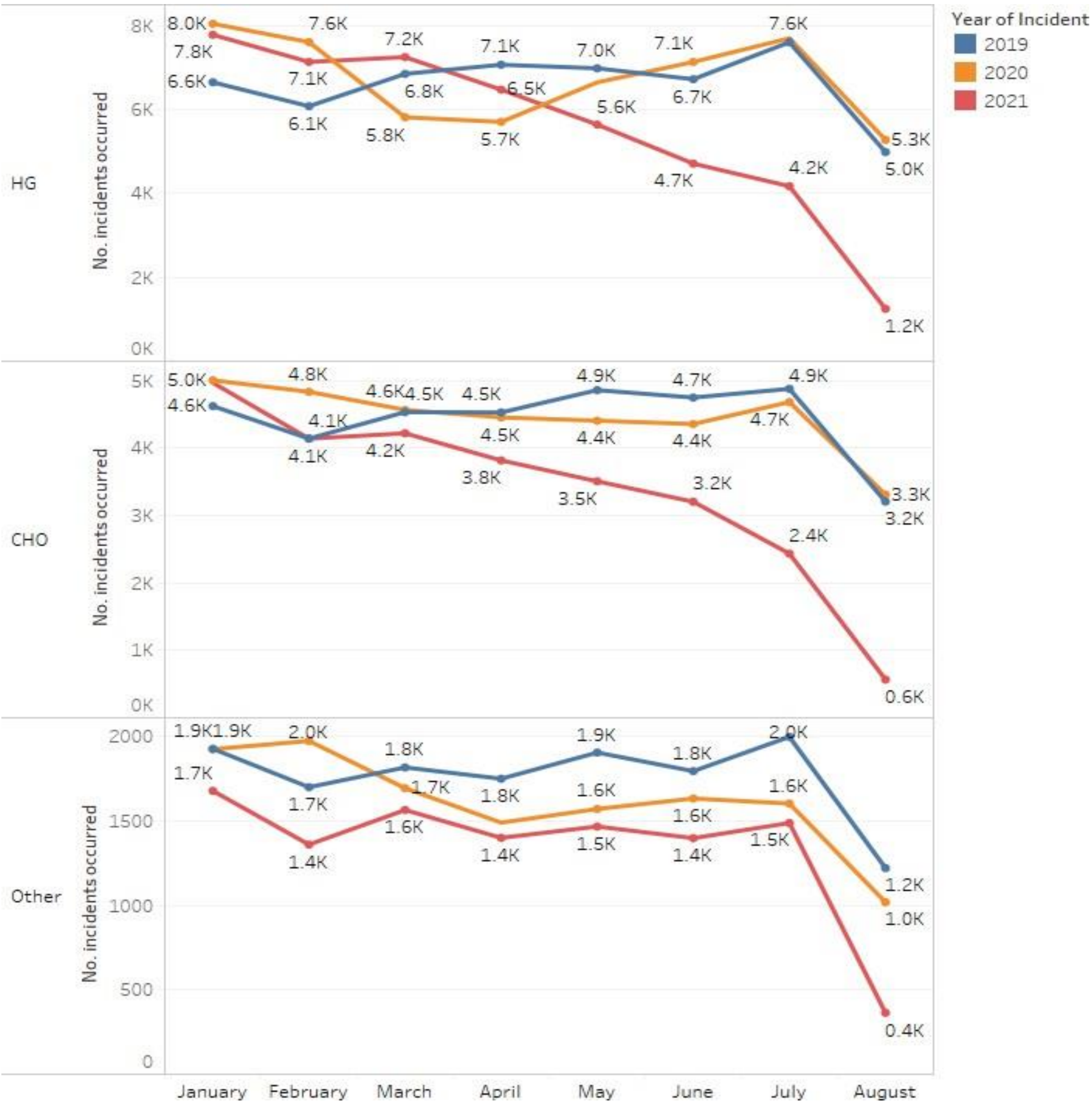
4.1.1. Incident analysis findings

Following the cyber-attack on 14 May 2021 access to NIMS was disabled for all health and social care users as a precaution. The findings presented in this section are based on the analysis conducted by the State Claims Agency (SCA) on incidents reported on NIMS after the HSE cyber-attack. The complete report is available in **Appendix File 5**. As of 23rd August 2021, the SCA estimated that 82% (n=4,683) of NIRFs received were uploaded to the system.

4.1.1.1. Quantitative findings

In comparing the number of incidents occurring in 2019 – 2021, from 1st January to 23rd August for each year, a 20% drop was observed from 2019 and 2020. An 11% drop in the incident report date data was noted in comparison with the previous two years. Based on the date of incident, there was a clear trend of a decrease in incidents occurring in 2021 from April, with a significant further drop in July/August. 2019 and 2020 had almost identical totals for the year to 23rd August (**See Figure 4.1**). The August numbers being the lowest month for 2019 and 2020 was due to only incidents up to the 23rd of August being included. The largest drop from 2020 to 2021 was seen for CHOs at just 18.1% of the 2020 total being reported, compared to 22.6% for Hospital Groups, and 40.0% for other locations. This drop was partially due to the standard reporting delay.

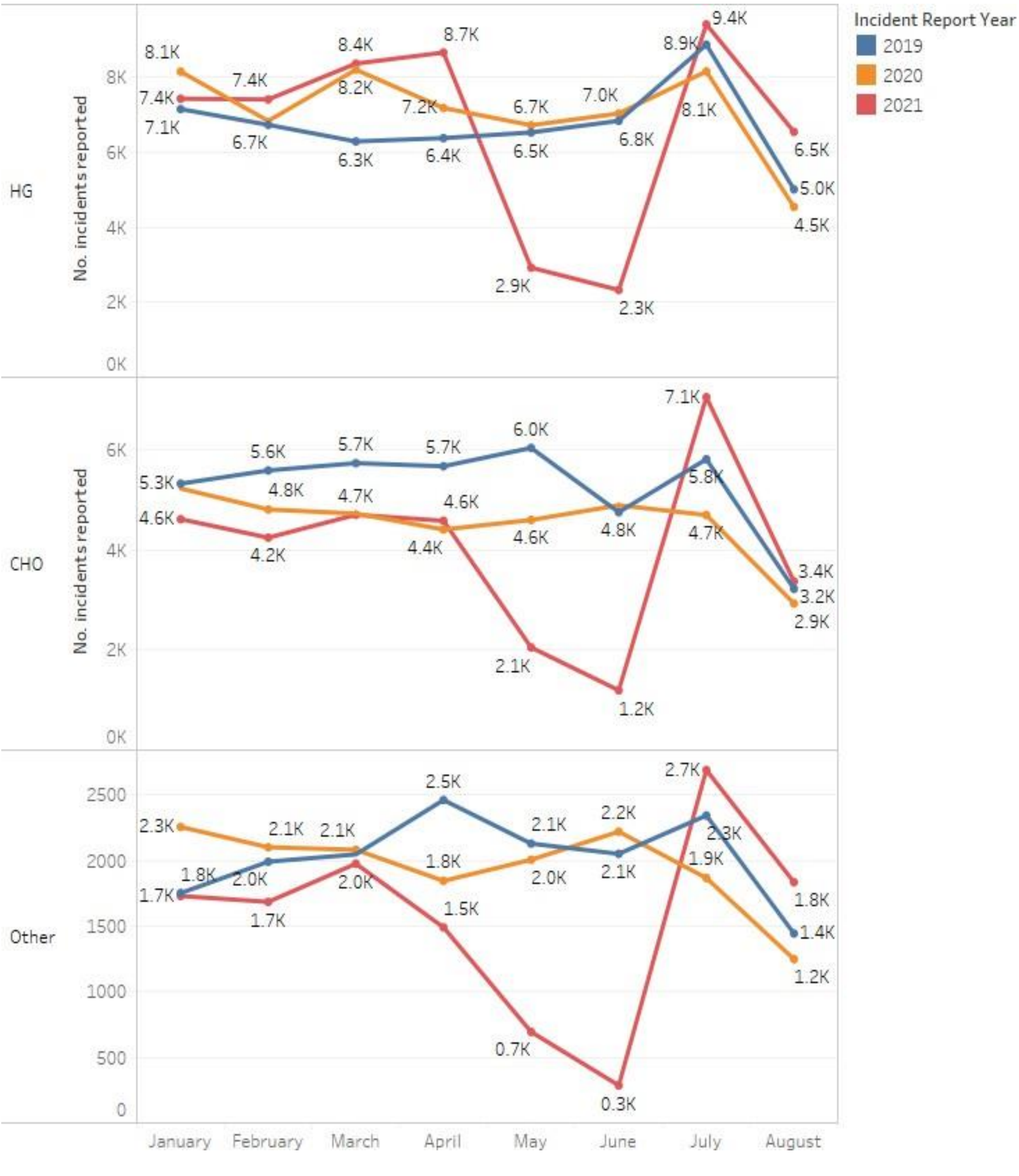
Figure 4.1: Number of Incidents in 2019-2021 to 23rd August each year, by month



Note: *'Other' locations include all locations which are not in a Hospital Group or CHO Area, e.g., National Social Care, National Services and Community.*

There was a clear drop in incidents reported for May, when the cyber-attack occurred, and June for the year 2021. This was followed by the highest reporting totals of any month in July for all locations. The reporting for Hospital Groups in August was up in 2021, by 30.1% on 2019 and 44.0% on 2020. For Hospital Groups, 2021 had the highest total of reported incidents in April 2021, compared to 2019 and 2020. While Hospital Groups had higher number of incidents reported year to date in 2020 compared to 2019, it was the opposite for CHOs and 'Other locations', which were slightly higher in 2019. **Figure 4.2** presents the number of incidents reported during this period.

Figure 4.2: Number of Incidents reported in 2019-2021 to 23rd August each year, by month



Note: *'Other' locations include all locations which are not in a Hospital Group or CHO Area, e.g., National Social Care, National Services and Community*

NIMS was reopened on June 24th, 2021. Looking at only the incidents occurred from 1st July to 23rd August all locations had a drop off in 2021 compared to the two previous years. In total, Hospital Groups were down 58.2%, CHOs are down 62.5% in 2021 from 2020, and other locations down 29.4%. The number of incidents reported from 1st July to 23rd August 2021 increased for Hospital Groups (up 25.6% on 2020), CHOs (up 36.7% on 2020), and other locations (up 45.2% on 2020). When comparing Hospital Groups and CHO's reporting from 1st July to 23rd August in 2021 compared to the same period in 2020, sixteen hospitals showed a decrease while 3 CHO Areas showed a decrease in number of incidents reported from 1st July to 23rd August for 2021 compared to the same period in 2020. There was an increase in incidents recorded from 1st July to 23rd August for 2021 compared to the same period in 2020 for both HSE and SCA users. HSE users reported 13.8% less in 2020 than 2019 but in 2021 reported the highest total of the 3 years.

4.1.1.2. Qualitative outcomes

The themes identified, in descending order of frequency, along with more detailed information on each theme, are presented below. Given the small number of incidents in this sample, the relative frequency of incidents should be treated with caution:

Table 4.1: Qualitative themes from incident analysis

Theme	**Brief Description**
No access to IT systems	Inability to access critical systems which impacted administration, communication, lack of access to teleconference facilities for medical consultation, access to lab findings and other functions
No access to healthcare records	There was no access to healthcare records or medical history, unrecoverable loss of patient records
Impact on provision of care	Cancellations, delays in treatment, diagnosis, procedures, services and delayed triage and referrals
Service user identification	Incorrect service user identifiers on documentation and theatre lists and no access to barcoded wristbands
Manual systems workarounds	Manual workarounds led to transcriptional errors, data protection issue and samples and forms with incomplete information
Documentation issues	Incorrect Healthcare Records, incorrect service user identifiers, illegible handwriting, forms missing important information and misfiling or records
diagnostic imaging	Suboptimal image quality
Cyber security	• There was an increase in unsolicited phone calls, requests for credit card details and potential data breaches after the cyber-attack

4.1.2. Content analysis of risk register

Due to the Cyber Attack, standard process for recording risks on local risk register were disrupted and as a consequence new methods of recording and escalating risks were established. In practice, this was achieved through two processes:

- Operational governance stood up meetings with a corresponding risk register and

- Clinical teams stood up meetings with a corresponding risk register

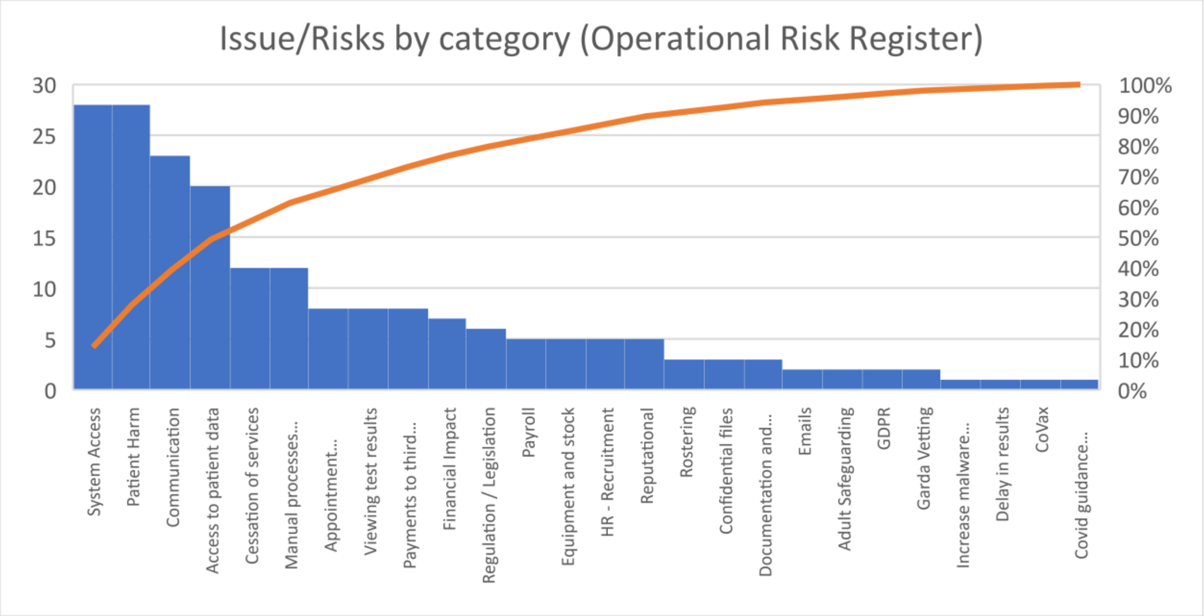
As the risk registers were administered separately, the analysis below is conducted on each register individually; however both suites of information informed the integrated operational/clinical governance team

Risk registers for operational and clinical meetings were stood up in response to the cyber-attack from 16/05/2021 to 08/06/2021 were analysed for frequency of reporting of risks across categories and business areas in categorical data fields and for word frequency and sentiment in free text fields. The Operational Risk Register classifies risks by category and Care Group/Business Area. It also presents a risk rating (0-25) calculated by multiplying risk likelihood (0-5) and level of impact (0-5). Three descriptive free text fields for Issue/Risk description (Brief), Issue/Risk Impact description and Action/Mitigation are provided. The Clinical Risk and Issue Register classify risk by Care Group/Business Area, Area and Category. It provides two descriptive free text fields Issue/Risk description and Comment/Mitigation. Levels of the Care Group/Business Areas variable and category variables in the two risk registers differ slightly but have many common levels.

4.1.2.1. Risk Categorisation

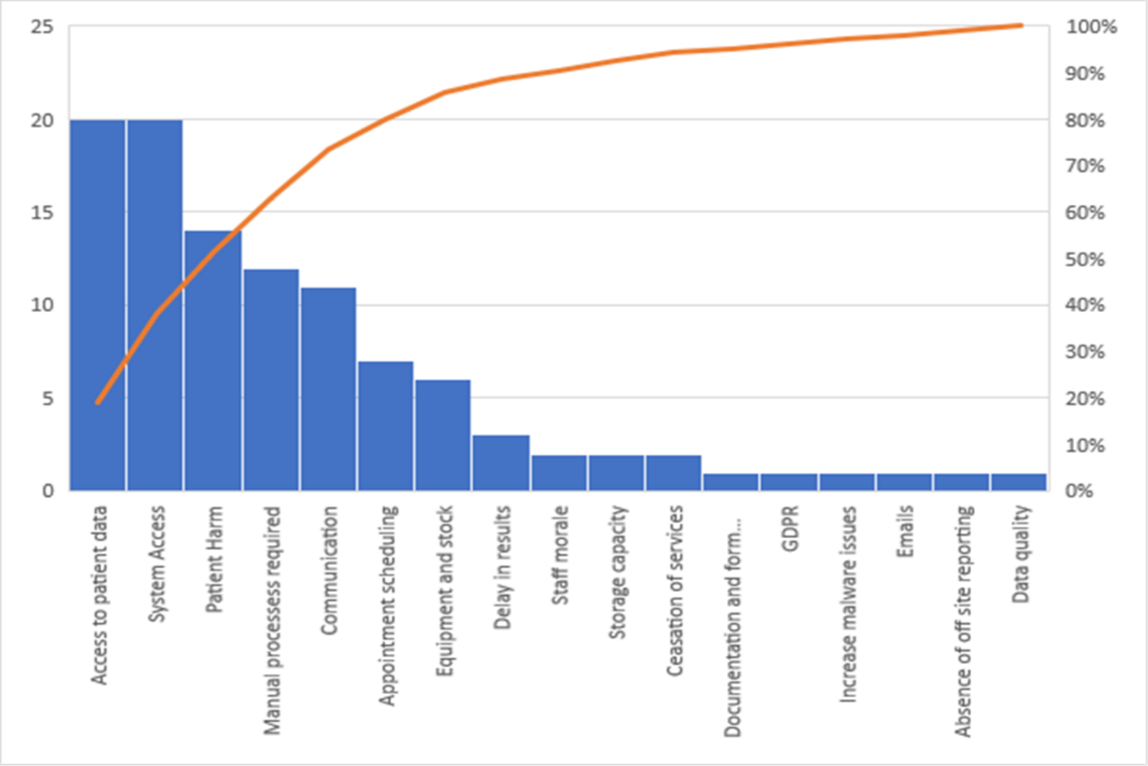
Looking first at the operational risk register, 201 risks were categorised in 26 categories during this period. Most reported concerns were system access (14%); patient harm (14%), communication (11%), access to patient data (10%), cessation of services (6%) and manual processing required (6%). All other categories accounted for 4% or less or reported risks/issues each (**Figure 4.3**)

Figure 4.3: Pareto Chart of Risks Category (Operational Risk Register)



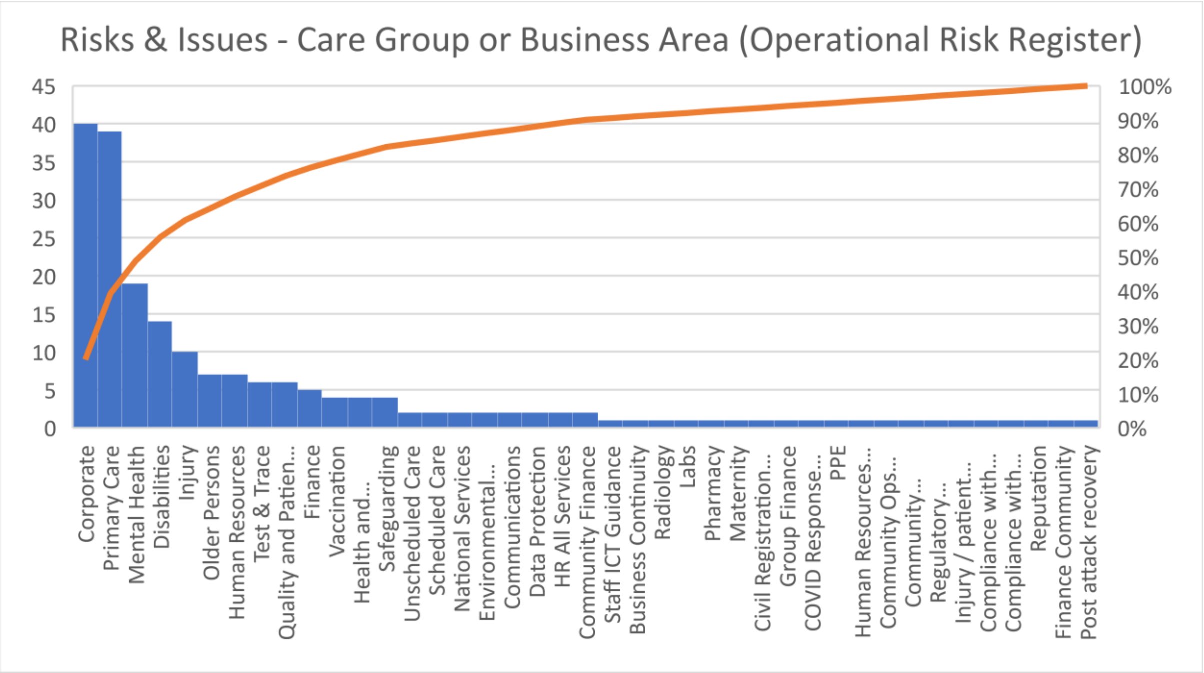
Secondly, examining the Clinical Risk Register, during the reference period, 105 clinical risks were classified into 17 categories. The most prevalent categories were access to patient data and System access, accounting for 19% of risks each. Patient harm (13%), Manual processes required (11%), Communication (10%), Appointment scheduling (7%) and Equipment and stock (6%) were also common risk categories. Other categories account for 3% or less of risks each **(Figure 4.4).**

Figure 4.4: Pareto Chart of Risk Categories (Clinical Risk Register)



Within the Operational Risk Register, of the 201 risks, 20% were recorded in the corporate business area, 19% in Primary Care, 9% in Mental Health, 7% in Disabilities, 5% in Injury, 4% in Older Persons, 4% in Human Resources and 3% in both Test & Trace and Quality and Patient Safety **(Figure 4.5)**

Figure 4.5: Pareto Chart of Risk/issue Care Group or Business Area (Operational Risk Register)



The average risk rating for non-zero-rated risks was 17.2 out of 25. Categories with the highest average risk rating were Patient Harm (20.25), Access to patient data (20.25), System Access (19.11), Regulation/Legislation (18.5) and Manual processes required (18.25). The average risk ratings are presented in **Table 4.2.**

Table 4.2: Risk frequency and average rating (Operational Risk Register)

Category	Count	%	Risk Rating
Patient Harm	28	13.93%	20.25
Access to patient data	20	9.95%	20.25
System Access	28	13.93%	19.11
Regulation / Legislation	6	2.99%	18.5
Manual processes required	12	5.97%	18.25
Viewing test findings	8	3.98%	17.5
Equipment and stock	5	2.49%	17.5
Cessation of services	12	5.97%	17.33
Garda Vetting	2	1.00%	15.5
Communication	23	11.44%	15.36
Payroll	5	2.49%	15
HR - Recruitment	5	2.49%	15
Emails	2	1.00%	15
Reputational	5	2.49%	14.67
Appointment scheduling	8	3.98%	14.5
Payments to third parties	8	3.98%	14

Financial Impact	7	3.48%	12
Rostering	3	1.49%	12
GDPR	2	1.00%	12
Confidential files	3	1.49%	-
Documentation and form access	3	1.49%	-
Adult Safeguarding	2	1.00%	-
Increase malware issues	1	0.50%	-
Delay in findings	1	0.50%	-
CoVax	1	0.50%	-
Covid guidance adherence	1	0.50%	-

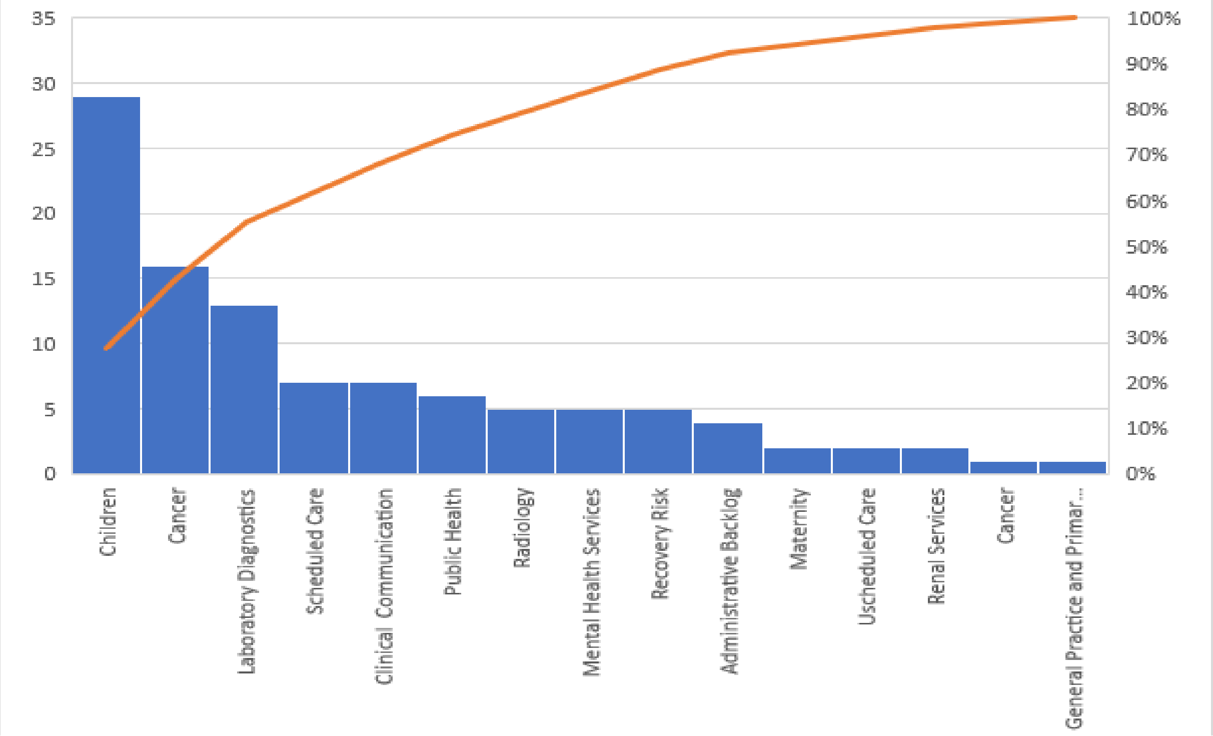
Within the Care Group/Business areas for which most risk/issues were raised, the areas with the highest average non-zero risk ratings were Mental health (22), Primary Care (19.86) Disabilities (18.42), Older Persons (15.75), Quality and Patient Safety (15.75), Human Resources (14.67) and Corporate (14.6). In the Mental Health Area, the highest rated risks were for access to patient data, communication, equipment and stock, and Patient Harm. In Primary Care, access to patient data, communication, manual process required, patient harm and viewing test findings were deemed to be the most significant risks. In disabilities access to patient data and patient harm were the top rated. In Older Persons the highest rated risk was Patient harm. In quality and patient safety and Human resources system access risks rated highest.

Table 4.3: Risk Rating by Business Group/Care Area and Category (Operational Risk Register)

Risk/issue Category	**Mental Health**	**Primary Care**	**Disabilities**	**Older Persons**	**Quality and Patient Safety**	**Human Resources**	**Corporate**
Access to patient data	**25.00**	**20.00**	**20.00**				17.33
Appointment scheduling		14.50					
Cessation of services		18.50	15.00				
Communication	**25.00**	**25.00**	15.00	15.00	10.00	9.00	16.00
Equipment and stock	**20.00**	15.00					
Financial Impact							12.00
Garda Vetting						15.00	
GDPR							12.00
HR - Recruitment						14.67	
Manual processes required		**20.00**			14.00		
Patient Harm	**25.00**	**22.50**	**25.00**	**25.00**			14.00
Reputational							16.00
Rostering							12.00
System Access	18.67	18.50	17.00		**25.00**	**20.00**	
Viewing test findings		**25.00**		8.00			12.00

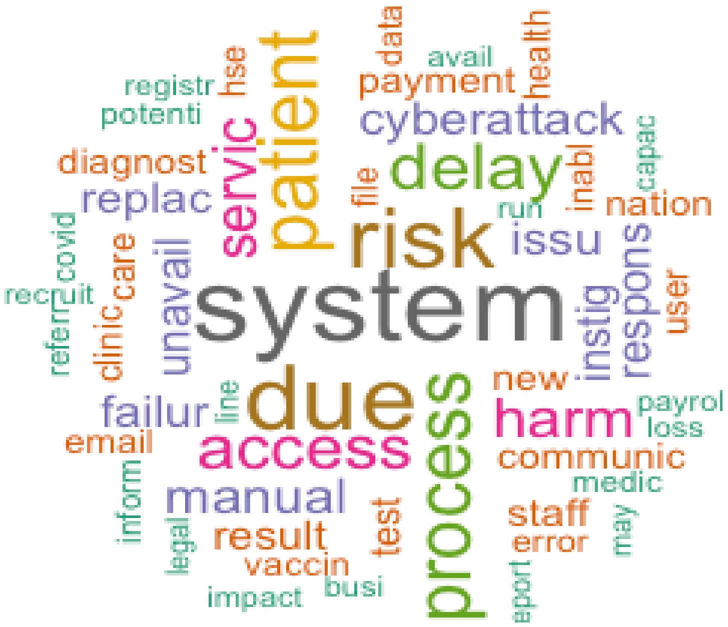
Within the Clinical Risk Register, the 105 risks were also classified by Business Area or Care Group. Children accounted for 28% of risks, Cancer 15%, Laboratory diagnostics 13% scheduled care 7%, Clinical communications 7%, Public Health 6%, and Radiology, and Mental Health Services and Recovery Risk 5% each. The risks were also classified by Area, which did not appear to have predefined levels. This meant that there were 64 areas levels with 51 representing just 1 risk. 16 risks (15%) were deemed to apply to all Areas, 7 (7%) to Laboratory, 5 (5%) to Radiation Oncology, 4(4%) to Scheduled Care and Child Protection and 3 (3%) each to Diagnostics, Critical Care and Clinical deterioration. All other risks Areas occurred only once or twice accounting for 57% of risks **(Figure 4.6)**.

Figure 4.6: Pareto Chart of Risks by Care Group or Business Area (Clinical Risk Register)



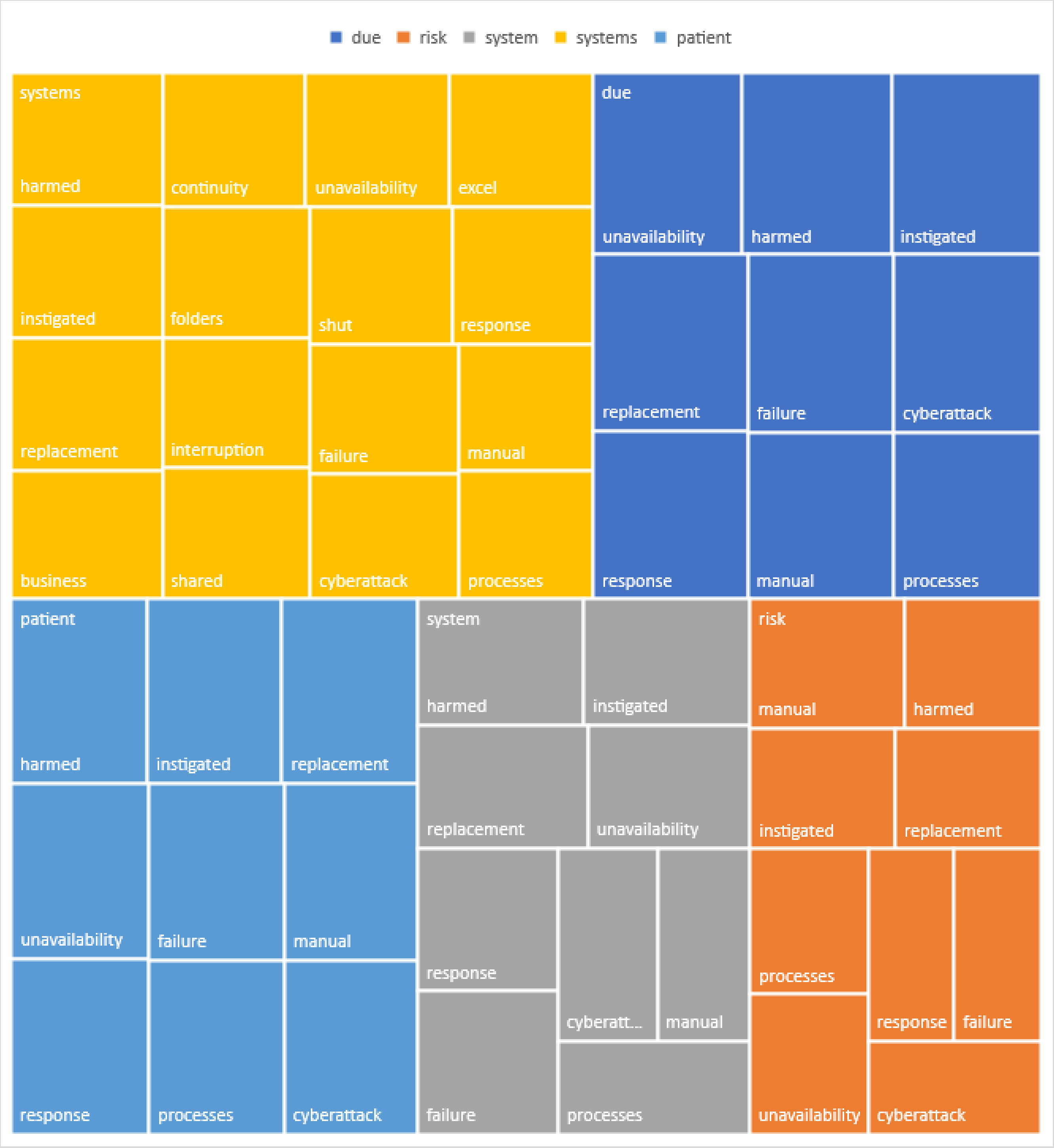
Within the Operational Risk Register there were three free text description fields. The first describes the risk or issue, the second describes the impact of the risk and the third the mitigation of the risk. Word frequency in the description of risk highlight concerns around systems, patients, processes, delays, access, and harm **(Figure 4.7)**.

Figure 4.7: Word Frequency-Operational risk register



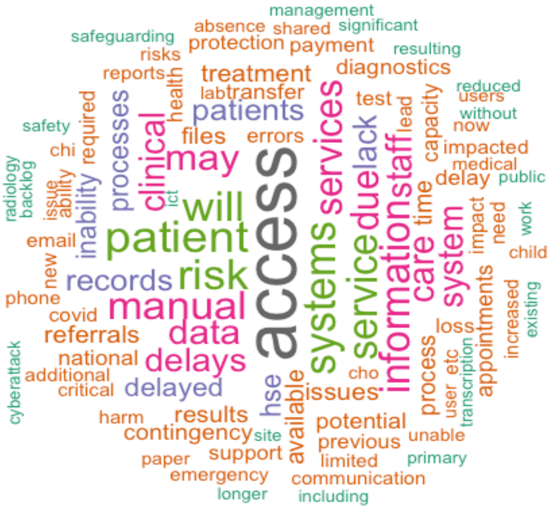
Correlations of commonly occurring co-located words with the top 5 most frequently occurring words indicated business continuity, access to folders and files and manual processes were the most frequently cited risks associated with downed systems **(Figure 4.8)**. Harm, and manual processes were of frequent concern because of delays. Harm and failure were the most cited words in association with patients. Overall, the requirement for replacement (of systems and processes) was a common theme.

Figure 4.8: Description of risk -Top 5 words correlation over 0.5 (Operational risk register)



Word frequency analysis of the impact of the risk-free text field indicated that access, services, systems, patients, and delays were frequently cited in the discussion of risk impact **(Figure 4.9).**

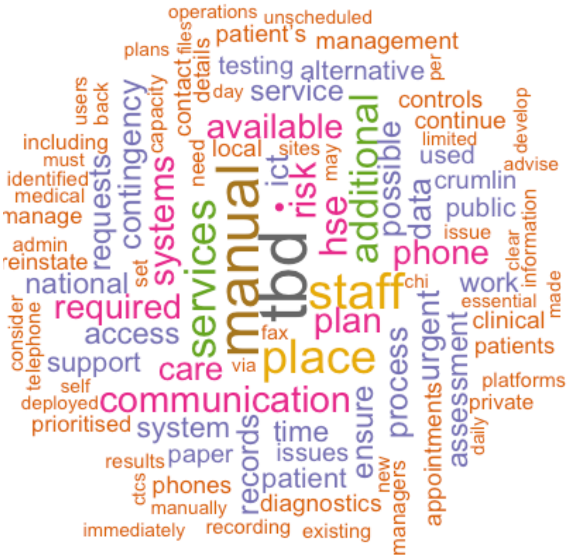
Figure 4.9: Word frequency- impact of the risk (operational risk register)



Reviewing word pairs that have a correlation of over 0.5 within the most frequent 5 words indicated that impacts to patients were focused around handwritten and nonstandard records, handwritten lab labels and wrist bands, difficulties creating new charts, unavailable records, and systems to view previous information, inability to add alerts and track Infection prevention control status.

Manual process impacts included concerns around processing and resulting of samples, refrigeration and temperature control, identification processes, accessing records, MRN generation for new-borns, interpreting handwritten records, delays, and risks of harm. Word frequency analysis of the mitigation of risk-free text field indicated that mitigations were often to be determined (TBD) **(Figure 4.10).**

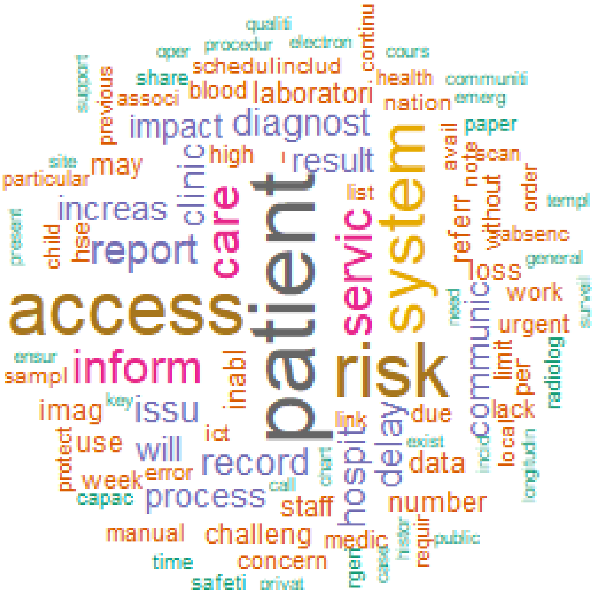
Figure 4.10: Word frequency – Mitigation of risk (operational risk register)



Mitigations also focused on manual process, additional staff and changes to services and communications. Word pair analysis with correlations of over 0.5 in the top 5 most frequent words indicated that changes to systems, radiotherapy, dialysis, scheduled and unscheduled care, assessments, diagnostics, laboratory process, and transfusions were commonly required. Alternative recording methods, operational and continuity plans, co-ordinators, documentation, devices, and meetings were put in place. Staff support was provided, and overtime was required.

Word frequency analysis of the description of mitigation/comments field and word correlations in the clinical risk register indicated that mitigations were required throughout the services. It also highlighted that cancer programmes (NCCP) and haematology required strong mitigation.

Figure 4.11: Word frequency - Description of risk (clinical risk register)



Reviewing word pairs that have a correlation of over 0.5 within the most frequent 5 words indicated that access issues were widely experiences across databases, emails, files, systems, and hardware resulted in impacts on clinical care, administration, training, recruitment, research. Lack of access to information and systems were associated with many diagnostic risks. Risks concerning care often related to dispensing and pharmacy as well as ordering. Risks around data breaches and statutory and regulatory requirement breaches were also common.

Word frequency analysis of the description of mitigation/comments field and word correlations indicated that mitigations were required throughout the services. It also highlighted that cancer programmes (NCCP) and haematology were areas which required strong mitigation.

4.1.2.2. Harm

The operational risk register and the clinical risk register both have harm as a categorisation. Areas which were most frequently associated with patient harm risk were Children's health, laboratory Diagnostics, cancer, maternity, unscheduled Care, public health, infection prevention and control and access to Care. The risks associated with patient harm exhibited the following common themes:

Theme 1: Access to information

- Risk of suboptimal clinical decision making due to lack of
  - Patients' medical history
  - Patients' current diagnostic information
- Absence of bed management systems impacting clinical handover, patient tracking and location
- Lack of access to child protection events
- Inability to track and trace infections and Covid-19

Theme 2: Delays

- Risks of patient harm due to delayed diagnoses, tests – pathology, radiology, haematology
- Delays in providing radiation oncology treatment
- Cancellation of electives
- Delays in issuing of prescriptions
- Delays in providing STI treatment
- Blood transfusion cross match delays

Theme 3: Manual Process

- Errors due to manual processes
- Transcription errors causing harm to patients
- Medication safety – errors in prescribing and dispensing

Theme 4: Children's health

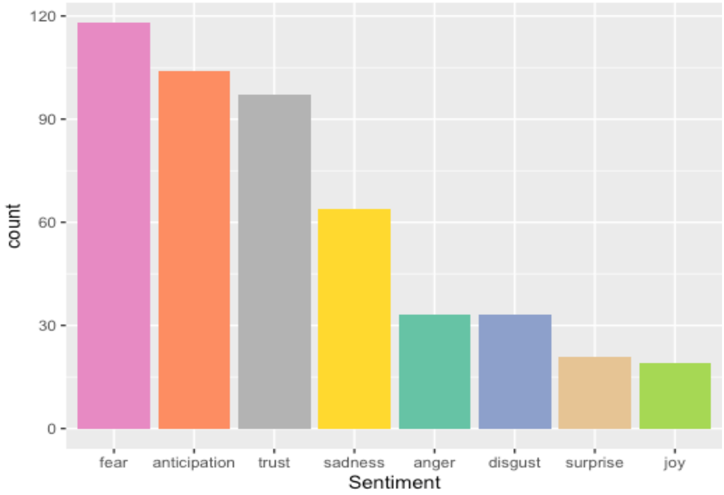
- Extracorporeal membrane oxygenation (ECMO) and sickle cell programme patients
- Heel Prick Screening suspension

4.1.3. Sentiment analysis

4.1.3.1. Sentiment analysis-operational risk register

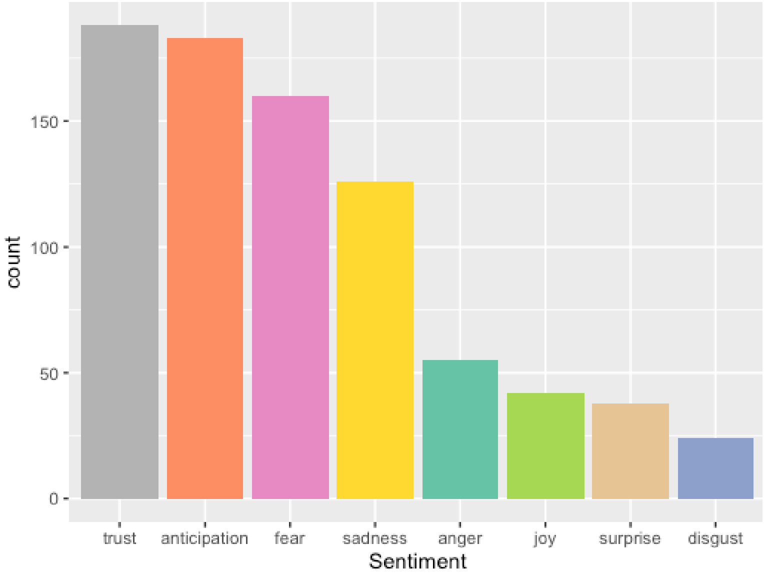
Sentiment analysis of the short description free text field indicated that fear was the dominant emotion expressed in the description of risk. This was followed by anticipation, trust, and sadness. Anger and disgust were also present, with low levels of surprise and joy **(Figure 4.12).**

Figure 4.12: Risk short description sentiments - operational risk register



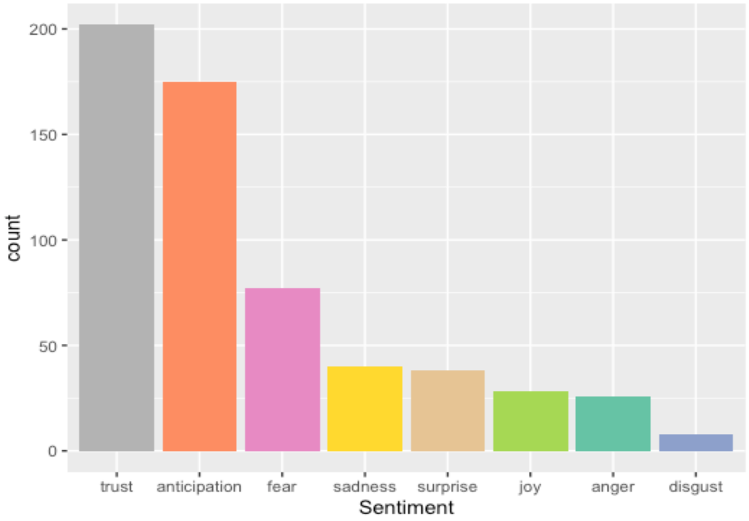
Sentiment analysis of the impact of the risk-free text field indicated that trust and anticipation were the most common emotions expressed, followed by fear and sadness. This contrasted with fear being the dominant emotion in the description of risk. Anger was also present, with lower levels of joy, surprise, and disgust **(Figure 4.13).**

Figure 4.13: Risk impact sentiments - operational risk register



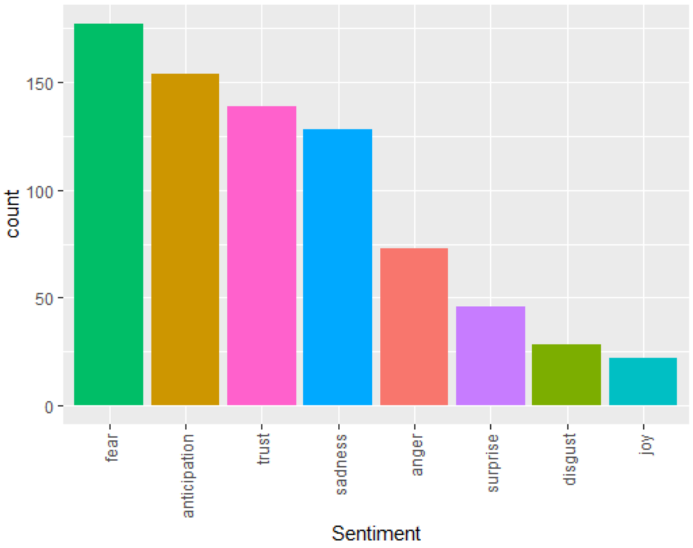
Sentiment analysis of the mitigation of risk-free text fields indicated higher levels of trust and anticipation than in the risk description and risk impact fields. It also showed much lower levels of fear and sadness. Surprise and joy were present at similar levels. Anger was also exhibited at lowers levels, with very minimal levels of disgust **(Figure 4.14).**

Figure 4.14: Mitigation sentiments-operational risk register



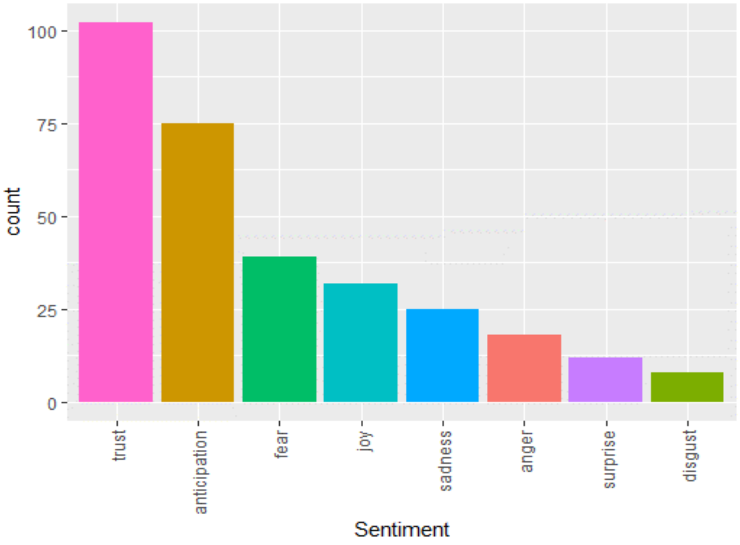
The sentiment analysis findings of the risk description and mitigation/comment free text fields in the Clinical Risk Register follow a similar pattern to that of the Operational Risk register. The description fields fear and anticipation were the most prevalent emotion, with high levels of trust and sadness. Anger was next most prevalent, followed by surprise, disgust, and joy in lower levels **(Figure 4.15).**

Figure 4.15: Risk description sentiment – clinical risk register



The Mitigation/comment field exhibited high levels of trust and anticipation, like the operational risk register. It also exhibited much lower levels of fear than the risk description. Joy and sadness were the next most prevalent emotion, followed by low levels of surprise and disgust **(Figure 4.16).**

Figure 4.16: Mitigation sentiments– clinical risk register

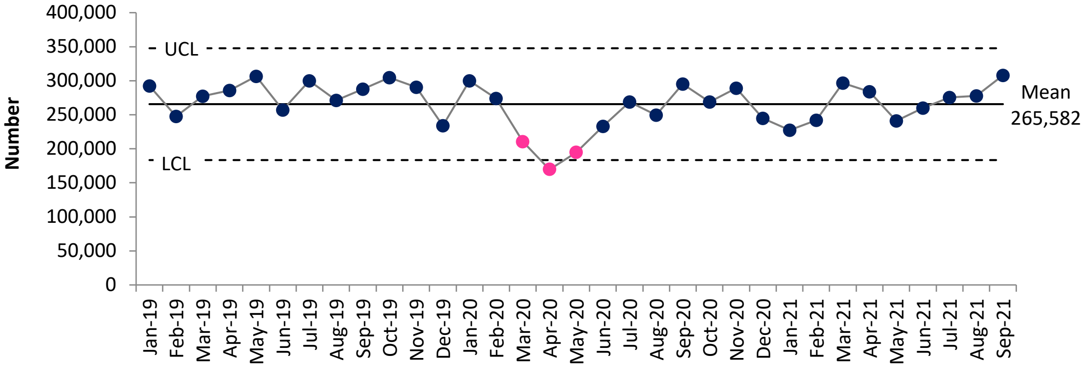


4.2. Work package 2 findings

4.2.1. Quantitative analysis of routinely collected indicators

An analysis of quantitative data related to activity in the Irish health system to determine the impact of the cyber-attack commenced in September 2021 and was updated with the latest available data in November 2021. In addition, several quality indicators were also analysed. Data are analysed and displayed using statistical process control (SPC) methodology, with unexpected variation in the data highlighted in pink. While interpreting the findings it is important to remember that a change that is not statistically significant may still be clinically significant. The findings are as follows:

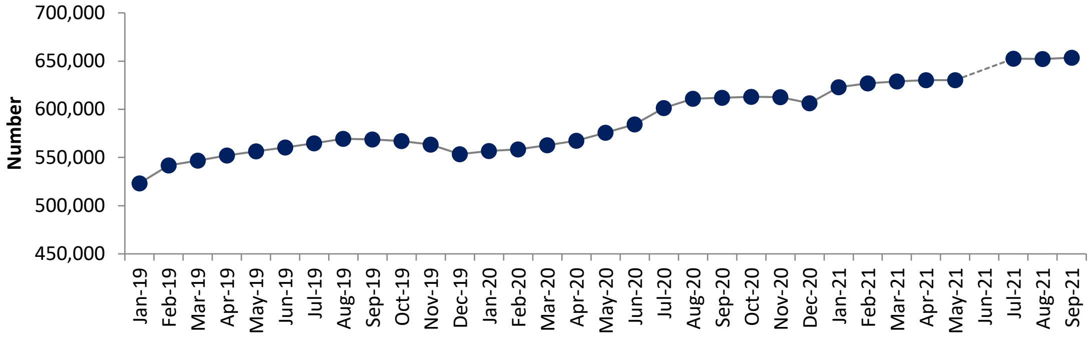
Figure 4.17: Number of new and return outpatient attendances



Between January 2019 and February 2020, the average number of outpatient attendances was just over 280,000 per month. This decreased to 210,370 in March 2020; down around 25% from normal levels and attendances remained lower than expected in April and May 2020. Attendances increased during the second half of 2020 and appeared to be returning to near normal levels. There was a drop in attendances again in January 2021 and February 2021 due to the surge in COVID-19 infections during those months, although this was within the expected range of variation using SPC methodology. Attendances in March and April 2021 were back to the level seen during March and April 2019.

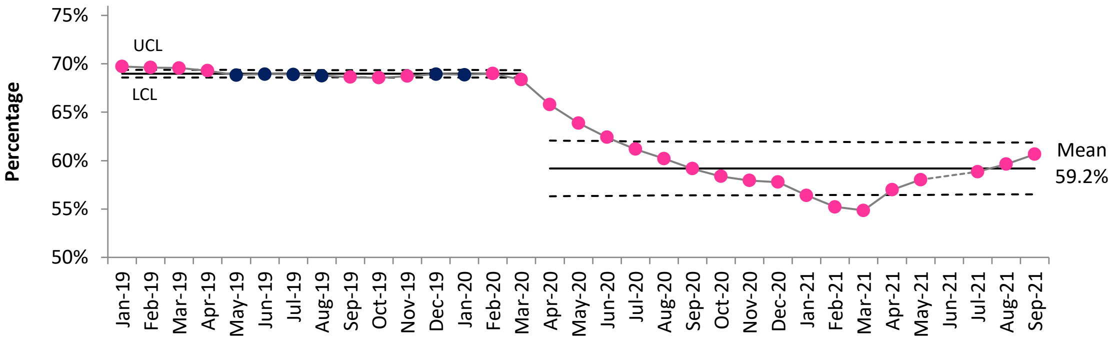
Following the cyber-attack there was no data on outpatient attendances for several hospitals for several months, although many of these data gaps have since been filled (May 2021: missing data for 3 of 49 hospitals; June 2021: missing data for 2 hospitals; July 2021: missing data for 1 hospital August 2021: data available for all hospitals). The number of reported outpatient attendances in May 2021 fell to 240,949; down 15% on April 2021 and down 21% on May 2019. Attendances in June 2021 increased slightly (up 8% on May 2021) and were similar to June 2019 (up 1%). Outpatient attendances increased in July, August, and September 2021, and were higher than the level seen during the same period in 2020 (up 6%) and similar to the same period in 2019 (up 0.3%). However, using SPC methodology, the number of attendances has remained within the expected range since June 2020.

Figure 4.18: Number of people waiting for a first appointment at a consultant-led Outpatient clinic



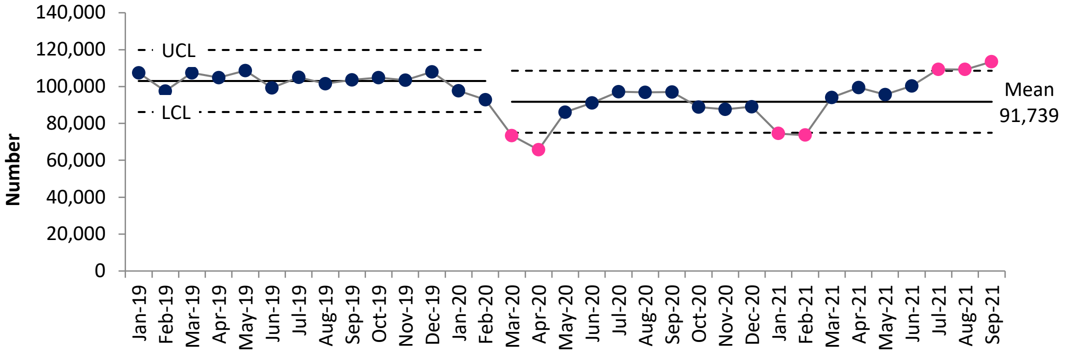
The number of people waiting for a first appointment at a consultant-led outpatient clinic has trended upwards since January 2019. Due to the cyber-attack the number of people waiting in June was not available. Data for July 2021 showed a continuation of the upward trend. However, the increase between April and July 2021 (+22,193 people, +3.5% increases in total number waiting) was greater than the increase between January and April 2021 (+7,342 people, +1.2% increases in total number waiting).

Figure 4.19: Percentage of patients waiting <52 weeks for first access to OPD services



The percentage of patients waiting less than 52 weeks for first access to outpatient services trended downwards since the beginning of the pandemic. However, this trend changed in April 2021, and since then the percentage of patients waiting less than 52 weeks for first access to outpatient services has improved. There was no data available for June 2021 due to the cyber-attack; however data for July 2021 showed that the upward trend continued.

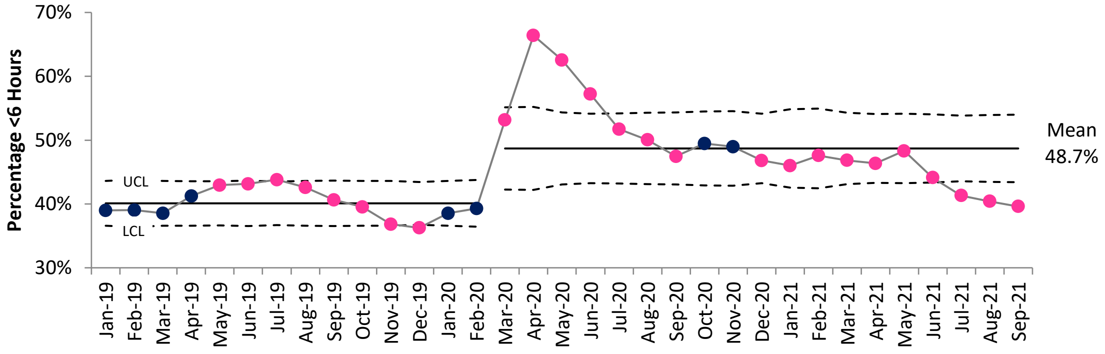
Figure 1.20: Number of new emergency department (ED) attendances



Between January 2019 and February 2020, the average number of new emergency department attendances was 103,000 per month. This decreased to a low of 65,706 in April 2020; down around 36% from normal levels. Attendances increased during the following months but remained below normal levels prior to the cyber-attack (attendances in April 2021 were down 5% on April 2019). The control limits in the SPC chart above have been recalculated to reflect this change.

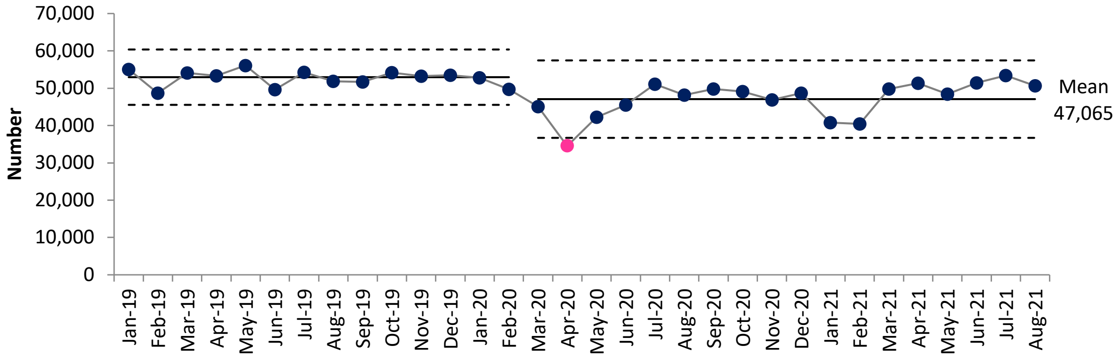
The number of ED attendances reported in May 2021 decreased by 4% compared to April 2021; however the SPC analysis shows that this decrease was within the expected range of variation for this data. ED attendances increased since May 2021, and for July, August and September 2021 were higher than expected. Note that data for 4 of the 30 hospitals remains missing for May and June 2021, with data was also not available for 1 hospital in July 2021.

Figure 4.21: Percentage of all attendees aged 75 years and over at ED who are discharged or admitted within 6 hours



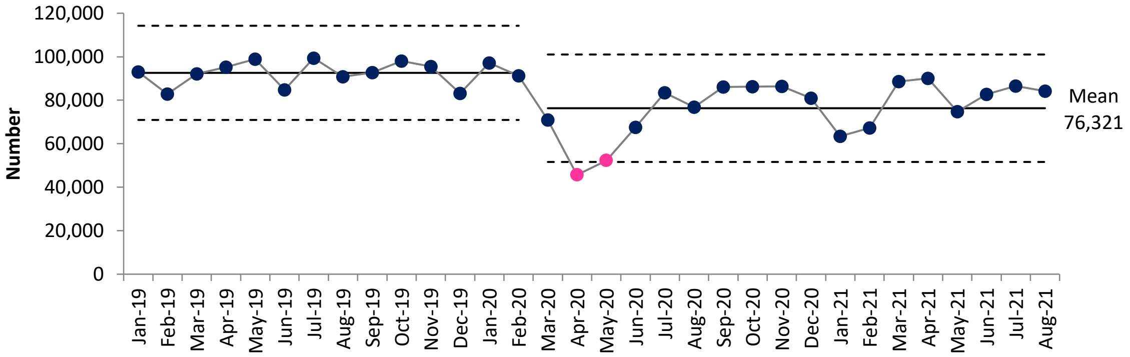
There was a significant improvement in the percentage of all attendees aged 75 years and over at ED who were discharged or admitted within 6 hours in the early months of the pandemic. However, this was followed by signals of dis-improvement, although the level remained above the pre-pandemic average. The percentage of all attendees aged 75 years and over at ED who were discharged or admitted within 6 hours improved slightly in May 2021 compared to the previous month, but this was within the range of variation expected for this data. Overall, there are signals of dis-improvement in this data since December 2020 (10 consecutive months below average), with additional signals of dis-improvement in the most recent 4 months.

Figure 4.22: Number of inpatient discharges



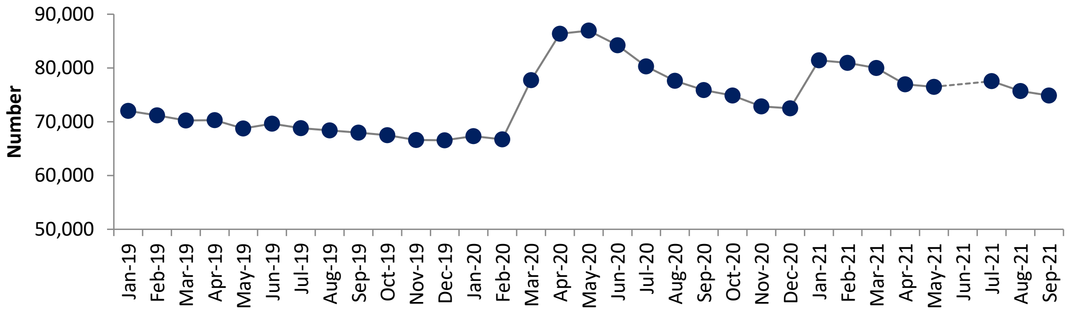
The number of inpatient discharges decreased from an average of 52,951 between January 2019 and February 2020 to an average of 47,065 since March 2020 (a decrease of 11%). The number of inpatient discharges has remained stable at this lower average since March 2020, except for April 2020 which was lower than expected. The number of inpatient discharges decreased in May 2021 compared to April 2021 (down 6%), although the SPC analysis shows that this was within the range of variation expected for this data.

Figure 4.23: Number of day cases (including dialysis)



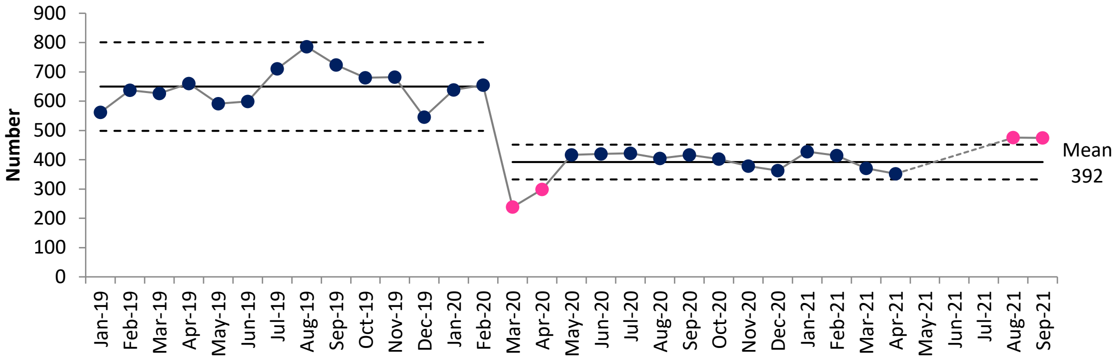
The number of day cases decreased from an average of 92,587 between January 2019 and February 2020 to an average of 76,321 since March 2020 (a decrease of 18%). The number of day cases has remained stable at this lower average since March 2020, except for April and May 2020 which were lower than expected. The number of day cases decreased in May 2021 compared to April 2021 (down 17%), a larger reduction than the decrease in the number of inpatient discharges during that month. However, the SPC analysis also shows that this was within the range of variation expected for this data.

Figure 4.24: Inpatient & day case active waiting list



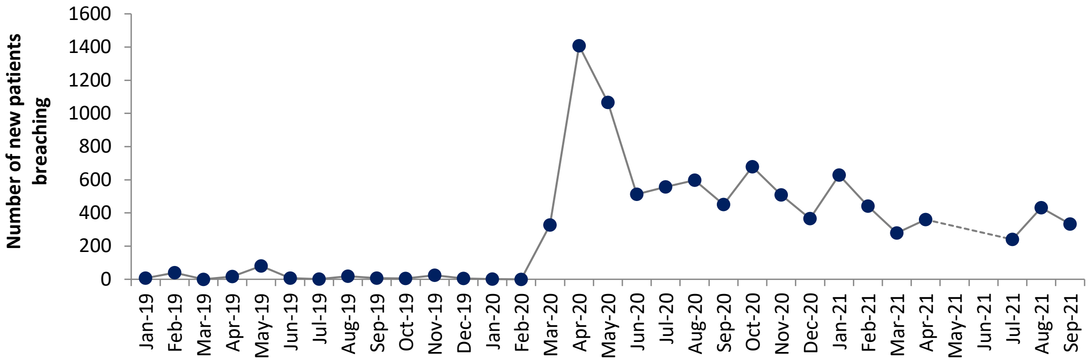
The number of people on the inpatient and day case active waiting list has fluctuated considerably since 2019. Following a significant rise during March and April 2020, the number had trended downwards until December 2020. The number of people on the waiting list increased in January 2021 but then trended downwards up until May. There is no data available for June 2021 due to the cyber-attack, but data for July showed a slight increase in the number of people on the waiting list in comparison to May 2021 (+1,027 people, +1.3% in the total number of people on the waiting list). The number of people on the waiting list subsequently decreased in August and September 2021, and it appears that the downward trend has resumed.

Figure 4.25: Number of delayed transfers of care



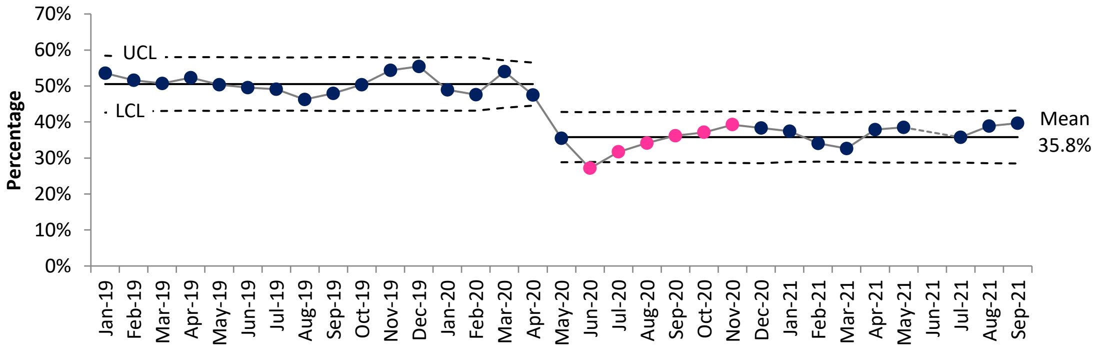
Between January 2019 and February 2020, the average number of delayed transfers of care (delayed discharges) was 650. In March 2020 the number fell to 238. It increased since then to 417 in May 2020, but between May 2020 and April 2021 remained stable at an average of 380, significantly below the average prior to the pandemic. Due to the cyber-attack data on delayed transfers of care were not available from 11th May until 31st August. Data for 31st August and September 2021 showed that the number of delayed transfers of care was above the upper control limits of the SPC and was therefore higher than expected.

Figure 4.26: Number of new people waiting more than four weeks for access to an urgent colonoscopy



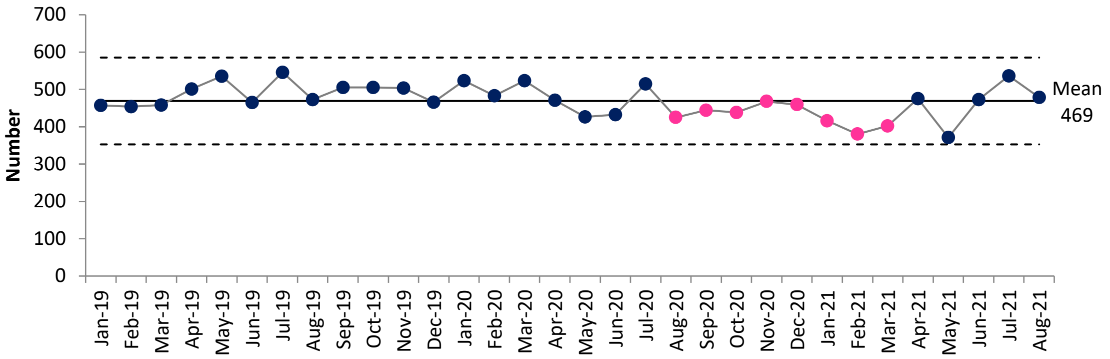
The average number of new people breaching the four-week target for access to an urgent colonoscopy between January 2019 and February 2020 was 15 per month. This increased considerably during the early months of the pandemic, and although the number of breaches decreased since then they have remained at a high level. There is no data available for May and June 2021 due to the cyber-attack; however data for July, August and September 2021 showed similar numbers of breaches to the previous 3 months (February, March, and April 2021).

Figure 4.27: Percentage of patients waiting <13 weeks following a referral for routine colonoscopy or OGD



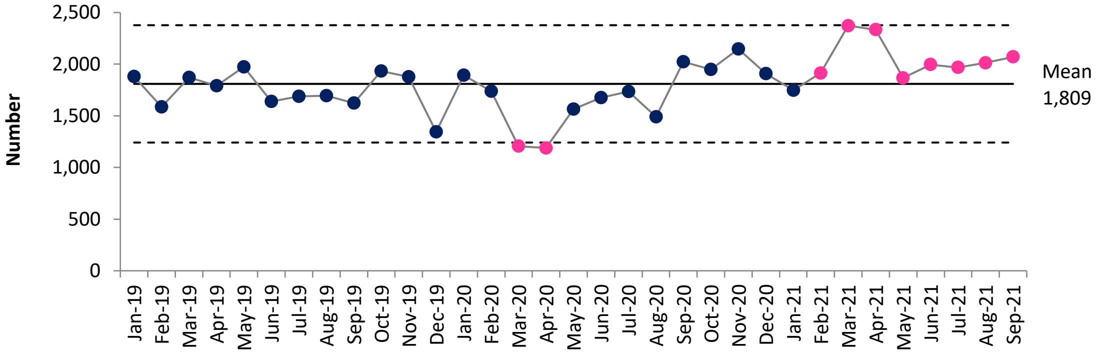
The percentage of patients waiting less than 13 weeks following a referral for routine colonoscopy or OGD decreased from an average of 50.5% between January 2019 and April 2020 to an average of 35.8% since May 2020. There was a signal of improvement between June and November 2020 (a series of 6 consecutive months during which the rate increased), but this trend was not sustained. There is no data available for June 2021 due to the cyber-attack. Data for July 2021 showed a slight reduction compared to May 2021, followed by slight increases in August and September. However, these month-to-month changes were within the variation expected for this data.

Figure 4.28: Number of patients who completed radical radiotherapy treatment (palliative care patients not included)



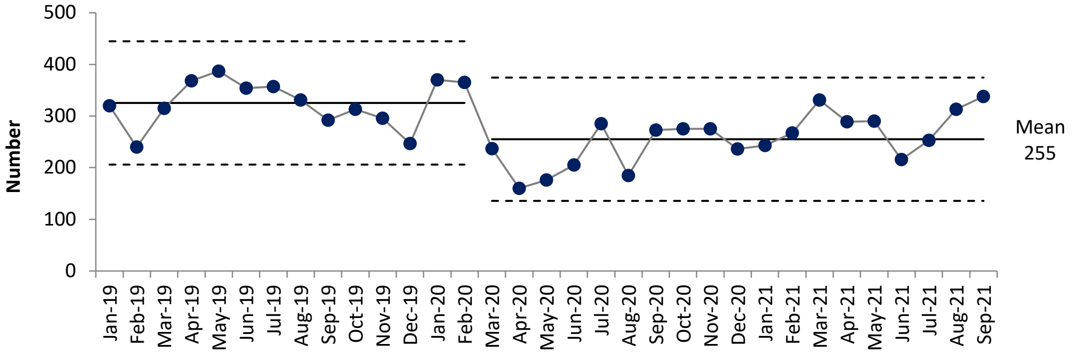
Statistical process control analysis shows that the number of patients completing radical radiotherapy treatment initially remained stable during the pandemic, but between August 2020 and March 2021 the number of patients was below average for 8 consecutive months. Using SPC rules this is a signal of unexpected variation, in this case a lower number than expected. This signal resolved in April 2021, when the number was above average. There was a decrease in the number patients completing radical radiotherapy treatment in May 2021 compared to the previous month (May 2021 was down 22% on April 2021, with no missing data). Activity increased in June 2021, and was up 27% compared to May 2021, and increased further in July 2021. However, the SPC analysis shows that these month-to-month changes were within the expected level of variation and were not significant.

Figure 4.29: Number of patients triaged as urgent presenting to symptomatic breast clinics



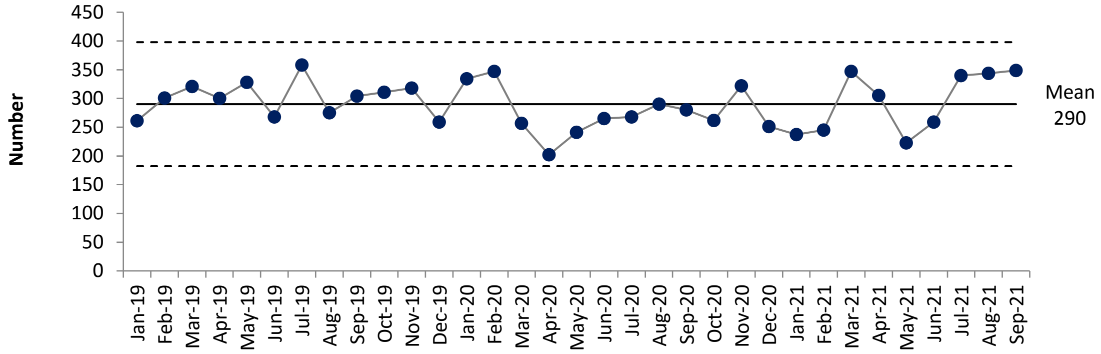
The average number of patients triaged as urgent presenting to symptomatic breast clinics since January 2019 is 1,809 per month. There was a signal of unexpected variation in March and April 2020 with a lower number of patients than expected. However, the number of patients returned to normal levels between May 2020 and January 2021. Since February 2021 the number of patients has been above average for 8 consecutive months, which using SPC rules is a signal of increase. While the number of patients decreased by 20% in May 2021 compared to April 2021 it remained above average.

Figure 4.30: Number of patients attending rapid access prostate clinics in the cancer centres



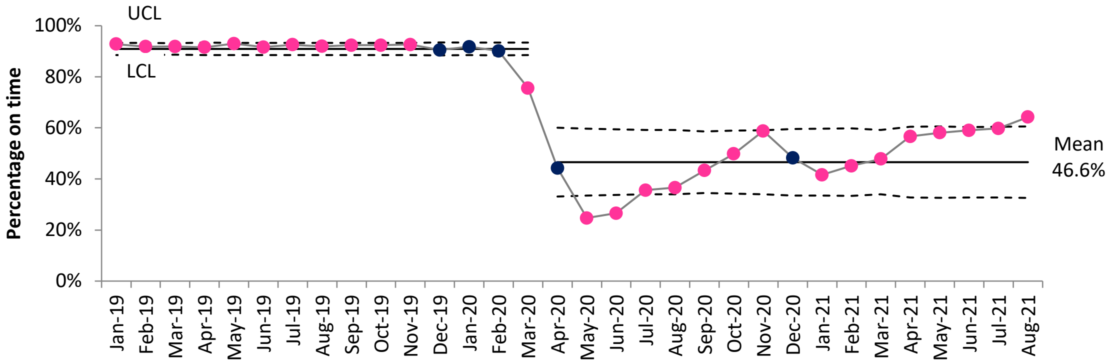
The average number of patients attending rapid access prostate clinics was 325 per month between January 2019 and February 2020. There has been a sustained reduction in the number of patients since March 2020, with an average of 255 patients per month. The number of patients in May 2021 was almost unchanged compared to April 2021 (289 patients in April, 290 in May 2021), and the month-on-month variation since then has been within the expected range.

Figure 4.31: Number of patients attending rapid access lung clinics in the cancer centres



The average number of patients attending rapid access lung clinics has been 290 per month since January 2019. This has remained unchanged since then, with no unexpected variation. While the number of patients in May 2021 was down 27% on April 2021, this was within the expected range of variation for this indicator.

Figure 4.32: Percentage of child health & development assessments completed on time or before 12 months of age



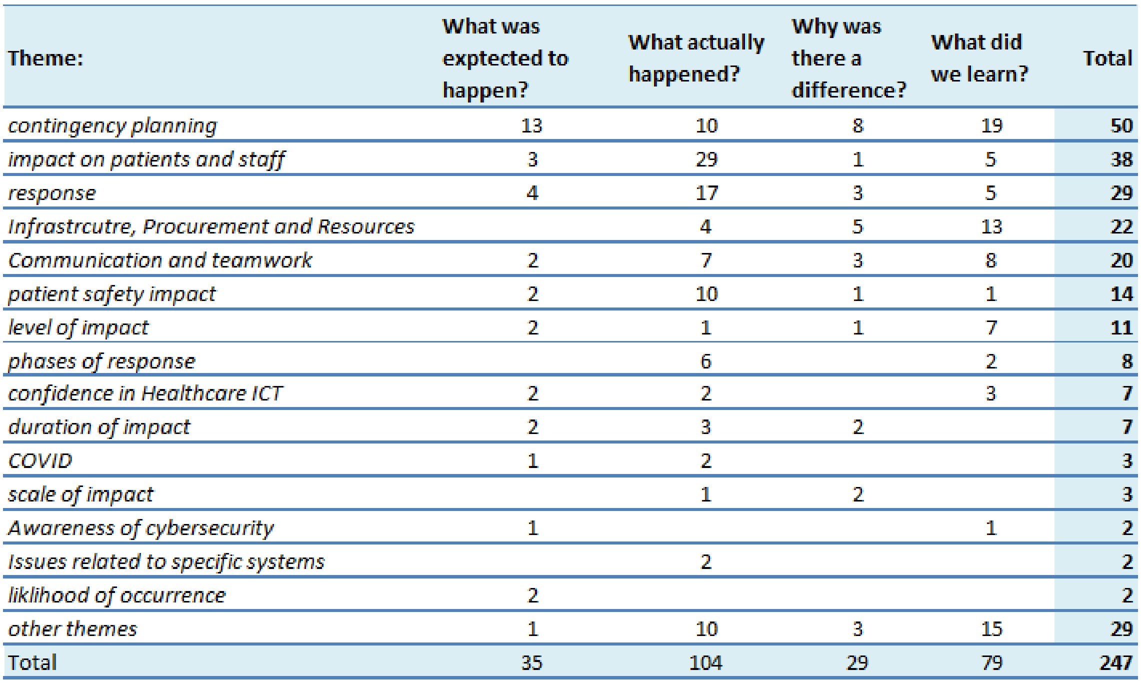
Between January 2019 and March 2020, the average percentage of child health & development assessments completed on time or before 12 months of age was 91%. There was a significant reduction since the beginning of the pandemic to an average of 46.6% since April 2020. However, there are currently signals of improvement since January 2021, including a series of 8 consecutive months during which the rate increased. This upward trend has continued in the months since the cyber-attack.

4.3. Work package 3 findings

4.3.1. AAR findings

Services are in the process of completing After Action Reviews. Many services have identified this as an action following their own reviews of the impact of the cyber-attack. Detailed AARs are presented in **Appendix Files 6a, 6b, 6c** while **Table 4.4** summarises the data from AARs:

Table 4.4: Frequency of themes



Theme:	What was exptected to happen?	What actually happened?	Why was there a difference?	What did we learn?	Total
contingency planning	13	10	8	19	**50**
impact on patients and staff	3	29	1	5	**38**
response	4	17	3	5	**29**
Infrastrcutre, Procurement and Resources		4	5	13	**22**
Communication and teamwork	2	7	3	8	**20**
patient safety impact	2	10	1	1	**14**
level of impact	2	1	1	7	**11**
phases of response		6		2	**8**
confidence in Healthcare ICT	2	2		3	**7**
duration of impact	2	3	2		**7**
COVID	1	2			**3**
scale of impact		1	2		**3**
Awareness of cybersecurity	1			1	**2**
Issues related to specific systems		2			**2**
liklihood of occurrence	2				**2**
other themes	1	10	3	15	**29**
Total	35	104	29	79	**247**

The following themes emerged across acute and non-acute services and are worth considering when services are revising or introducing contingency plans for ICT downtime events.

- **Theme: impact on patients, staff, and services:**

Participants felt that there was an association between the impact of the cyber-attack and the level of integration of healthcare information technology. Staff in non-acute settings routinely relied on paper-based systems including patient charts and it was felt that the impact would have been more profound in community settings had paper-based charts not been in common use. Staff commented that frequent transfer of patients between services is a feature of community care and in this scenario, the absence of patient histories and other clinical notes would have had significant impacts on services for patients and staff.

In contrast, in areas where ICT systems routinely support care processes and paper-based processes were not routinely used, staff felt that not having Laboratory, Pharmacy, Radiology or EHR systems had a significant impact on patient safety. Paper charts with detailed histories, diagnostics and notes were not available as a fall back in services that operate using an EHR. Some staff (clinical and non-clinical) had never worked in a paper-based system and had only trained in an electronic environment. Without the prompts and structure of the ICT systems, it was therefore difficult to ensure that all relevant information was recorded accurately and consistently on paper. Some clinical data was therefore not recorded and there will not be any opportunity to recover some information or fill in missing data when electronic systems are back online. It is likely that there may be patient safety impacts of the cyber-attack which will remain after all systems have been restored.

Some staff spoke of the damage that the cyber-attack has had on confidence among staff in the use of ICT systems in healthcare. With the planned further implementation of Electronic Healthcare Records (EHRs) in the Irish healthcare system such as the Maternity and Neonatal clinical management system (MN-CMS), some work is required to assure staff that learning from the Conti cyber-attack has resulted in more robust contingency planning for ICT system downtime. Additionally, AAR participants discussed the lack of awareness and training among staff in dealing with cyber-attacks. There was an assumption that staff had a certain level of IT literacy and would be able to follow instructions which proved to be untrue.

Specific examples of how patient safety was impacted are included here in summary:

Some staff reported that they had only worked and trained in digital environments where electronic health records or similar systems were in use. Reverting to paper alternatives, without the system prompts they were accustomed to, presented problems. It was concluded among AAR participants that some clinical and non-clinical information may not have been recorded within the appropriate timeframe. This was a key finding that was not reported in the literature review. The implication is that, despite the significant resource and effort used to backload clinical information following restoration of clinical systems, there will be some data that is irretrievable. The impact of the cyber-attack will therefore be long lasting and will affect clinical practice for some time to come.

The absence of system prompts for medication dosages was also reported as being a significant difficulty for prescribers. Where paper charts and documentation were introduced, staff reported that the hard copy layout of the charts or documentation did not match the layout on electronic systems and it was concluded that over time, some divergence had been introduced. In addition, staff reported that paper charts from other similar services may have been locally adapted. This resulted in difficulties in ensuring a consistent single format of paper-based documentation were in use for all patients and service users.

There was a reliance on patient's recollection of relevant history in the absence of access to clinical notes. For example, in maternity services, findings of Group B Streptococcus tests may not have been available in all cases, and information may only have been available through patient's recall of findings. Manual writing on blood sample vials was reported where printed stickers or bar codes were not available. This introduced the risk of transcription error, or the wrong information being recorded. Accurate identification of patients and correct reporting of findings are fundamental to patient safety. Where pathology services were impacted, staff also reported that they had to prioritise which lab tests were most urgent to request. One group reported that this happened while patients were in operating theatres for example.

- **Theme: Duration and phases of the downtime event:**

In settings that have implemented significant ICT systems such as EHRs, there is usually a requirement to have contingency planning in place as part of the implementation process. This is in recognition that system downtime can be planned or unplanned. Planned downtime is usually no more than several hours and allows for system or hardware updates. Unplanned downtime not only includes cyber-attacks, but also natural disasters such as floods or fires in key ICT facilities or rooms or power outages.

In practice, there was consensus that the contingency plans in place were not adequate for a downtime event that lasted weeks. For example, one system took a download of key data fields in a read only format from the last 7 days. In practice during the downtime event, the dataset was not as useful as it could have been, and other more useful fields would have made a significant difference. As a contingency, the usefulness of such a dataset diminishes over time and in a service where the population of patients continually changes, after a week, the contingency dataset is largely obsolete.

Some staff identified three phases of the cyber-attack. The first few days were the most challenging as low technology processes were designed and implemented rapidly, and the scale of the downtime event became clearer. In answering the question 'What did you expect to happen', staff reported that they thought it was a possibility that systems would go down but did not expect the scale of the event to be so severe as to affect most systems or that essential equipment like networked phones and photocopiers would be affected. The duration of the event was far longer than their expectations. These points are relevant for contingency planning as staff felt that where contingency plans existed, they were mainly designed with a downtime event of up to a week in mind.

The second phase identified was where paper based systems and other low technology systems were in use. It was felt that staff were innovative and flexible in rapidly implementing new processes in a short space of time. Some services still had fax machines in storage that could be reactivated as a communication channel to replace e-mail. Analogue phone lines were installed in key areas (e.g. pharmacy) and some pathology systems were accessible through a designated PC in clinical areas to facilitate clinician access to findings. For varying reasons, some individual ICT systems were able to function, and it was not unusual for a combination of paper and electronic systems to be in operation.

The third phase was when systems were restored, and a focus of this phase was the back loading of information and data that was recorded on paper or other means during the downtime event. This is time consuming work and for clinical systems and information, clinical staff are best placed to do this. The scale of the task should not be underestimated, especially in the context of the length of this downtime event. It is worth noting that in the article included in the literature review by Coffey et al (12), back loading of data took up to a week for a downtime event that lasted 33 hours. The three phases of the downtime event described here also correspond well with the phases described by Chen et al (16).

- **Theme: communication**

As a theme, communication was a key feature across all AARs. In this section we summarise the discussions at AARs of the initial communication to the services of the cyber-attack from central HSE. Many staff reported hearing about it first through media channels and in some cases, where communications were pushed down through the system, it did not reach senior clinical staff. This is relevant for contingency planning, and it is suggested that some consideration is given to maintaining lists of key staff that should be included in key communications should similar events occur in the future. In addition, participants felt communication was done differently on different sites and between different staff groups.

Without e-mail or networked phones as main communication channels, face to face communication and manual delivery of handwritten paper communications became commonplace. These workarounds did however pose difficulties for staff considering the risk of facilitating COVID-19 transmission. However, some staff also commented that many staff had been equipped with mobile phones as part of the COVID response, and this was invaluable for timely communication.

Communication with other agencies was also problematic because of the cyber-attack. Understandably, some agencies would not accept e-mail communications from HSE accounts, and a phone call was made to the HSE account holder to confirm details by phone. For example, a single notification to a regulator may result in several phone calls. Another knock-on effect of the inability to use HSE e-mail accounts was a delay in the GRO process which led to delays in child benefit payments for new births or delays in issuing passports.

4.3.2. Focus group findings

Over a four-week period in September and October 2021 eight focus groups were conducted with front line staff working in an acute hospital, a maternity hospital, and a community health area. Focus groups were conducted with teams consisting of multi-disciplinary colleagues with different roles including clinical, business management, scientists, administrators, and information systems. A description is provided in **Table 4.5.**

Table 4.5: Focus group details

Care Area	Focus group	Service type	Number of participants
Community	Focus group 1	Dental Services	2
	Focus group 2	Health and Wellbeing and COVID testing	4
	Focus group 3	Disability	3
	Focus group 4	Social Care – Older Persons	2
Acute	Focus group 5	Radiotherapy	8
	Focus group 6	Radiology	3
	Focus group 7	Laboratory Services	4
Maternity	Focus group 8	Maternity services	10
		Total participants	**36**

Focus groups were transcribed and thematically analysed. The key themes developed are presented under three sections: 1. the impact of the cyber-attack on continuity of services, 2. the mitigations implemented by healthcare teams and 3. the on-going challenges and concerns for the future.

4.3.2.1. Impact of the Cyber-attack on Continuity of Care

The impact of the cyber-attack varied among services depending on several factors including the type of care being offered, the reliance on software systems to record and manage patient data, existing IT infrastructures and local IT support. Community care services that were less reliant on electronic methods prior to the cyber-attack and those that were set-up independently from the main HSE network (COVID setup) were less impacted. However, the participants in acute and maternity services were completely reliant on electronic methods and were therefore more severely impacted. This highlights the variance in access to ICT systems and local IT support between acute and community settings.

Participants reported experiencing previous IT system downtimes, but these were either planned, partial and usually short, giving staff enough time to plan and continue normal services. The cyber-attack's duration was unprecedented and was a new experience for all staff. The backup systems contained basic patient data for the last 7-15 days and therefore quickly became irrelevant. The cyber-attack also impacted the ability of services to report on their KPIs, making payments to vendors and finalisation of policies, which may have indirect implications for patient safety. The theme of service disruption is presented in the following table with supporting quotes from the focus group participants:

Table 4.6: Theme 1: Service disruptions

Community	• Although there were delays, service-users were in the main still able to receive treatment and services • Services lost sight of which patients were scheduled for appointments, patient histories and treatment plans • The referral pathways through Healthlink between GPs and services were lost: *"All the clients or prospective clients got their test, but their challenge was their GP didn't get their finding, so it was all resulted back into public health, the department of public health medicine, so they then had to deal with the fallout of generating those reports back to GPs".* Participant C6
Acute	• The radiology, radiotherapy and laboratory teams were unable to access almost all their systems • The teams had no access to patient histories and treatment plans: *"It is easier to say we could access nothing. Weren't able to access our oncology information system, we weren't able to access our shared files; we weren't able to so be able to access the lab systems [...] No medical records for the patients on treatment or coming through the system*". Participant A3 • Staff had to make high-risk decisions based on limited information: *"We literally had only our memories to rely on – nothing else and we had to reconstruct very high dose radiotherapy, very complex treatment from memory so couple of things here there was a time issue there was an enormous lack of information".* Participant A6
Maternity	• The maternity service was fully digitised and lost access to almost all systems such as patient management, referral system, X-rays, ordering systems and neonatal labelling: *"Very little could happen safely, initially […] we had no clue as to the patients who are coming in. We had no idea of what their complaints were. We had no way of knowing had they had a previous surgery. Had they not with no way of knowing any histology that had been done"*. Participant M3 • Biochemistry findings are central to the work of maternity services and the cyber-attack reduced the capacity of labs to approximately 10% of the original: *"We were told we had only more than 10% of what the lab in biochemistry could perform for us. […] we had to determine off a paper list and not knowing what their history was and that was done in collaboration with the consultant and anaesthetist as to whether they needed a full blood count or do you decide at section, OK we need to cross match her".* Participant M4

Staff stepped up to the challenges and quickly developed and implemented innovative, effective and efficient solutions, exhibiting great resilience, teamwork, and adaptability with a sharp focus on ensuring patient safety. Their approach and dedication enabled the continuity of patient care in extremely difficult circumstance. However, participants reported that staff continue to experience high levels of stress, anxiety, and uncertainty as they deal with two concurrent challenges of the COVID-19 pandemic and the cyber-attack. One unexpected outcome from the community care focus groups was that in the absence of ICT systems, staff found more time to spend with service users in residential homes. Theme 2 presents the impact of the cyber-attack on the healthcare staff.

Table 4.7: Theme 2: The impact on healthcare staff

Community	• High levels of stress and fatigue observed among staff and frustration among service users • Staff were already suffering from immense fatigue owing to the COVID experience and the cyber-attack exacerbated the situation • Staff were also frustrated as they were unable to provide the level of services they wanted, due to the cyber-attack • Staff had to use their personal devices and work long hours due to manual processes: *"All my numbers got wiped, and I think I'd thought I'd cry that day, that was the ultimate low".* Participant C6 *"It was the pure helplessness and the inability to address it in a reasonable time".* Participant C7 *"On top of the pandemic for this to happen next you just thought what are we doing, it was soul destroying".* Participant C11
Acute	• Staff that were already exhausted by the pandemic were under significant pressure due to the cyber-attack and the additional work required to retrospectively enter data when systems resumed • Staff had to work long hours under stressful conditions: *"We were putting in 16 plus hour days, significantly more I think at the beginning and then the uncertainties that impacted that... I will say I still wake up at 4 in the morning in a cold sweat about what we did".* Participant A6 • Staff were constantly worried about whether they were treating patients correctly or not • The high-stress levels are reflected in increased sick leave and mental health issues among staff: *"It's had a huge impact or sick leave and has gone through the roof and it's down to things…certainly an increase in mental health issues and generally just being unwell and its long-term sick leave that we're seeing"*. Participant A3
Maternity	• The waiting lists were already growing due to COVID-19 and the cyber-attack worsened the situation leading to an increase in stress and feeling of helplessness among staff: *"It was the thing [Cyber-attack] crippling our healthcare for weeks. And we are now having to claw our way back to where we were like. We have been trying in our hospital to work on waiting lists and try and improve the quality and the timeliness of the service that we provide to our patients. COVID impacted on this, but the cyber-attack impacted even more on it".* Participant M3

	• The cyber-attack had a profound psychological impact on staff. Staff were at the receiving end of verbal abuse from service users despite trying their best in exceptional circumstances • Participants perceived the cyber-attack experience as being more challenging than the COVID experience: *"You hear colleagues saying that they would much rather take a global pandemic over a cyber-attack. You know that things are very, very bad".* Participant M3

4.3.2.2. Mitigations implemented

As the cyber-attack impacted their normal systems and practices, staff had to quickly adapt to the challenge and implement and refine mitigations rapidly to ensure continuity of services. This often involved developing manual paper-based systems and forms. Some common mitigations across the three areas included setting up Gmail accounts in the absence of HSE email, using personal phones and WhatsApp, conference calls, physically traveling to sites for meetings, using the postal service, asking patients through external communication/website to phone in ahead of schedule. The service specific mitigations implemented by staff are presented in the following table as Theme 3.

Table 4.8: Theme 3: Mitigations implemented

Community	• Some examples of manual workarounds implemented were: **Dental and orthodontics:** Asking the patients to phone in in advance, using old film x-rays and fax machines, manual tracing system for dental equipment sterilisation, using disposable equipment, using fax machines, **COVID Testing:** Opening additional COVID testing centres and using non-HSE labs for processing COVID samples, managing traffic outside testing centre, **Health and Wellbeing:** Texting people on a weekly basis to maintain engagement, postponing some programmes, delivering programmes online **Disability:** Manual duty roasters, photocopying forms and filling them manually, making calls to ensure sites had adequate funding, posting preliminary screenings to safeguarding team, sending, and receiving notifications with HIQA via post, manual invoice payments and reconciliation. **Social care:** Physically meeting hospital discharge coordinator bi-weekly to obtain patient referral information, calling all agencies individually rather than the usual single email.
Acute	• Some examples of mitigations implemented by acute services include: **Radiology:** Manually delivering paper reports to requestors, using printing film that has not been used for the past 20-30 years, pausing outpatient appointments, selectively saving information due to limited storage of equipment, sourcing external archive hard drives, using carbon-copy books to develop multiple copies, T-Pro outsource digital deck dictation facility, getting help from the Army to take an inventory of PCs. **Radiotherapy:** Redirecting patients to private institutions, extracting patient dosage information from the devices, contacting GPs to get copies referral letters, searching in shredding bins for referrals or

	paperwork, Monday to Friday services working on weekends, radiobiology calculations to assist the doctors in informing prescriptions, using a new app for communication called Silo. **Laboratory services:** Manually entering patient information in the instruments and using manual systems to prioritise urgent samples, pausing the processing of GP blood samples, manually delivering reports and findings around the hospital, writing everything in paper and transcribing findings, manual forms with reference ranges.
Maternity	• Some mitigations implemented by maternity services include: Calling GPs and asking them to fax through referral letters and patient details, detailed hand-outs for processes, contacting other hospitals to obtain charts, outpatient appointments postponed for patients deemed low risk, taking detailed histories from patients manually, training staff to handle paper-based program charts, collaborating with a university to print memos

4.3.2.3. Current and future challenges posed by the cyber-attack

Service delivery, although limited, continued throughout the cyber-attack. However, there were various challenges described by focus group participants including rapidly developing, refining, and implementing mitigations and patient safety concerns that may arise in the future. Communication was identified as a critical element in the success of the cyber-attack response and staff discussed various barriers and gaps in communication that the teams faced (Theme 4).

Table 4.9: Theme 4: The role of communication

Community	• Participants suggested that communication targeting specific services and patients would be of benefit: *"People were hearing the acutes saying don't come [...] the public doesn't differentiate between services you know they just hear HSE services so that was very confusing whereas we could have been still seeing some patients you know"* Participant C2 • The 'Healthmail' accounts set up by the national office with each CHO to share information supported effective communication • Staff also struggled to understanding escalation pathways and who to direct their queries to • Participants reported that many patients were frustrated as they were unaware of the duration of the impact of the cyber-attack: *"A lot of verbal abuse from the public as well but despite it being a national cyber-attack there were members of the public who actually didn't know it".* Participant C6
Acute	• Regular and open internal hospital communication through formal and informal channels was instrumental in devising mitigations and discussing emerging issues:

	“There were crisis meetings twice a day that I would have attended, and the clinical directors were there as that feedback was given at that…like that instruction was given at that point”. Participant A12 - While the media initially reported on the cyber-attack it did not continue to do so as time progressed: “*It kind of dropped off the media and now I'm guessing they didn't focus on it too much in the media to feed into our hackers, all the rest of it.* Participant A11 - The participants stressed the value of regular communicating during such situations - Staff were uncertain about how to communicate with national IT
Maternity	- The uncertainty regarding the duration of the cyber-attack was challenging for frontline staff - Participants were frustrated by the number of manual templates required during this time

Community services described their limited access to IT systems and local IT support. While some services completely rely on electronic systems, others still rely on manual processes or have outdated systems in place. This highlighted the vulnerability of the health system to cyber-attacks and theme 5 summarises how this proved to be challenging during the cyber-attack.

Table 4.10: Theme 5: IT infrastructure and support

Community	• Local users were unfamiliar with the technical details of their systems : *“People (from IT) kept asking us for specific information about where things were on servers and where things were on PCs…sure we don’t know I mean I’m not in IT so I don’t understand what’s kept on what* • While some services had backup systems in place, these backups were designed for shorter ICT outages and due to the protracted nature of the event, the backups quickly became ineffectual. • Participants reported a lack of trust in IT systems the ability to protect against future events. • The cyber-attack highlighted what participants described as poor IT in community care systems *“there is a big gap in if you look at a comparable organisation in the private sector like their IT systems or their access is light years ahead of ours, like we are light-years behind”*. Participant C7
Acute	• The cyber-attack impacted trust of patient and service-users: *“It must have been totally discombobulating (for patients), you know, here nobody knows anything about me and I'm presenting myself for this serious illness I think I have.”* Participant A10 • The teams that had close relationships with their local IT support found it beneficial in understanding the emerging situation throughout the cyber-attack: *“We would have close ties with the there's a ICT department in X hospital which would be involved in PC and hardware replacement and we would have close ties and liaise with them and discuss any national information that they might have fed through their chief and would have a close link in with their line manager as well, so we were all working very closely to hope to try and get the best possible outcomes as quickly as possible, but also as safely as possible each way along, each step along the road”*. Participant A13 • The on-going impacts and risks are higher for legacy systems: *“Yeah, so most of the modern systems are back, but there are legacy systems that would have come say reports which we need to hold for 21 years for…there are maybe 10 or 12 years old, so we've moved on to new storage and they are not accessible still at the moment, so we have a variety of systems that are still not accessible”*. Participant A10
Maternity	• Participants would like more local IT staff on site to support their systems: • Participants felt there is scope to improve communication during IT downtimes: *“We had a downtime again during the week. We were down for…we thought we were going to be down for 24 hours again with our electronic chart, and again we didn't know what was after happening*

All focus group participants noted that the effects of the cyber-attack were on-going at the time of focus groups as teams wait for some systems to be fully functional and issues to be resolved. However, the experience has made teams more knowledgeable about the various risks facing their services. Even if the ICT systems are restored to full capacity, all risks cannot be eliminated. Participants were concerned that risks that emerged during the cyber-attack may only become evident in the future. Theme 6 discusses the various concerns highlighted by the focus group participants.

Table 4.11: Theme 6: On-going and future concerns

Community	• All services had not been restored completely, participants highlighted persisting issues such as glitches with the appointment system and no access to computers and VPN for some staff • Due to the manual workarounds enforced, the services are now focusing on retrospective data entry which may reveal gaps in the captured data and poses potential risks of data entry errors. This will require significant time and effort and should be considered while resource planning: "Our clinicians have recognised that people do need some protected time to put in that data, you know so that's kind of been built into the weekly rota and stuff as well". Participant C2 • Participants highlighted the need for learning to be consolidated across the healthcare system • Data privacy and safety is an on-going concern with a need for a reassurance to staff and patients that their data is safe • Participant noted a desire for further acknowledgement for the resilience, altruism and adaptability displayed by healthcare staff
Acute	• The participants stressed that the impact of the cyber-attack is on-going and various systems and processes have not been fully restored yet: *"You know everybody thinks we're back to normal and actually a week later it kind of dropped off the news and stuff, but we were really suffering energy and we continue…our productivity is very poor still from a digital point of view [...] It's really…so yeah, that's our estimate. Yeah, 30% productivity down and the digital side still".* Participant A9 • Many staff members are still not able to access their emails remotely which impacts flexible working • The cyber-security measures employed in response to the cyber-attack such as 'FireEye' have resulted in systems become slower and less accessible according to the participants. Various applications in use by the teams have been crashing more frequently • There is a large increase in equipment downtime as external support providers such as engineers can no longer remotely access equipment in many instances • As a huge volume of documents is being scanned into the system, participants were concerned about the quality of the data and its reconciliation with private institutions to which patients were re-directed

	"It is a long and convoluted process. We are still working on it, but we've just done majority of them. But that work is still going on so we need to import back to our system while working on the current training will work which is, you know increasing and so that that work is still on-going". Participant A2 • Detailed investigations and process have been established to ensure all data is captured and recorded • Old ICT systems are in use throughout the health system which have an increased risk to cyber-attack: *"Even our PCs here, we are Windows 7 based and we'd be hoping to move to Windows 10. And the speed at which the IT is replaced within the HSE is a big problem, IT hardware or even the planning for it".* Participant A13 • During the cyber-attack, participants reflected on their processes and identified the need for shedding non-value adding activities and streamlining the processes: "I think we've learned a lot and we've cut out a lot of time-wasting things". Participant A9 • Participants expressed concern that our health system may be on the brink of a staff mental health crisis and the risk of staff leaving healthcare services: *"I think we're at very high likelihood of losing a lot of staff both on long term sick leave, but also I can see an exodus from the health service once this has settled down a little bit".* Participant A6
Maternity	• Participants stressed that the risks from the cyber-attack and mitigations are on-going • There was a lot of concern about potential future incidents due to the risk of lost patient data and information during the cyber-attack; patient data during the time of the cyber-attack may not have been captured. Staff will have to be cautious in future while reviewing charts and data from this period • Retrospective data entry is a slow and tedious process which will take time • Staff suspect that they will not be fully aware of the impact of mitigations for a long time to come: *"It's a huge burden that people have to carry because we don't know what wasn't done. So, we can only hope that we captured all of the patients that weren't seen that need to be seen. We don't…We can't be certain. We don't have any kind of procedures in place to be able to follow this through, which is a very unnerving place to be when you're responsible for the health of a patient and particularly where time can be of grave importance in terms of outcomes".* Participant M3 • There is a decreased confidence and trust of staff in the current ICT infrastructure and reliance on electronic systems • Guidelines were developed for electronic systems and therefore there is an absence of similar guidelines for paper-based forms • Although staff tried their best to capture all information and risks, there is still a chance of missing information and data which will be an on-going risk for some time in the future: *"What's important to realise is that some of the things we did we might never capture. There was a loss of thinking on your feet, dealing with situations as they came up. Lots of individual,*

you know strategies and solutions put in place, so I'm not sure we'll ever capture on paper". Participant M9

- Participants were concerned about future planning for similar attacks or outages
- Due to the nature of the event, staff confidence in the ICT systems has been shaken.
- Staff were concerned that issues may emerge in relation to freedom of information and medical legal cases in future
- Pressures on healthcare staff will continue as the retrospective data entry has to be completed without additional resources

4.4. Summary of findings

The study objective was to complete a comprehensive analysis of the impact of the cyber-attack on patient safety including the impact on patient safety of the loss of key systems, the mitigations put in place and to capture key learning at both local and national level. The *research questions* that guided analysis were to explore the risk mitigation measures and contingencies required to safely deliver patient services and maintain health and social care services in the event of an either partial or complete Information Communication Technology outage and to identify what worked well and what needs to be improved. These research questions were answered using a literature review and a mix of qualitative and quantitative methods organised into 3 work packages.

The *incident analysis* based on the State Claims Agency (SCA) data revealed a clear drop in 'incidents reported' for May, when the cyber-attack occurred, and June for the year 2021. This is followed by the highest reporting totals of any month in July for all locations. This can be attributed to delays in reporting due to the cyber-attack. Similarly, there was a decrease in 'incidents occurred' data in July and August. The qualitative data in the SCA report highlighted issues including lack of access to IT systems and healthcare records and documentation issues due to manual work arounds.

Analysis of the risk registers classified the risks which are most prevalent and deemed to be the highest risk. It also identified the Business Groups or Care areas that have identified the most risk. Most frequently reported categories of risk were system access, patient harm, and communication, access to patient data, cessation of services, manual processing required and appointment scheduling. Business Groups/Care Areas and categories to interrogate further on this basis that reported high numbers of risks with a high-risk rating should include mental health (access to patient data, communication, equipment, and stock, patient Harm), primary care (access to patient data, communication, manual processes, patient harm and viewing test findings) and disabilities (access to patient data, patient harm). The clinical risk register had high frequency of risk reported in the business groups/ care areas of children, cancer services, laboratory diagnostics, scheduled care, critical care, and clinical deterioration.

The areas of concern identified by the text analysis of risk registers were transcription errors, handwritten lab labels, alternative record keeping methods, MRN generation for new-borns, radiotherapy, dialysis, transfusions, staff support, overtime, operational and continuity plans, data breeches, IPC alerts and refrigeration and temperature control. A further investigation of patient harm categories revealed access to patients' medical history and diagnostic information, bed management, patient tracking and clinical handover, tracking and tracing of COVID-19, delayed diagnoses, treatments, delayed blood transfusion cross matching, delayed prescriptions, manual process errors, medication safety errors, heel prick screening and ECMO and sickle cell programme as major concerns. Sentiment analysis of the risk register free text fields of both the clinical and operational risk registers identified significant fear and anticipation, however trust was also strongly present, as was sadness. When considering the describing of the mitigation of risks, a change was observed with trust and anticipation the majority emotions expressed with much lower levels of fear and sadness. These points to an initial fear response due to much unexpected circumstances with a great deal of uncertainty followed by building of trust as mitigations were identified and implemented.

Quantitative analysis of 16 routinely collected indicators revealed that the number of outpatient attendances during the cyber-attack remained within the expected range and there was a continuation of the upward trend in the number of people waiting for a first appointment at a consultant-led outpatient clinic. Data for July 2021 showed an upward trend in the percentage of patients waiting less than 52 weeks for first access to outpatient services. The number of ED attendances reported in May 2021 decreased by 4% however this decrease was within the expected range of variation. ED attendances increased since May 2021, and were higher than expected for July, August, and September. There have been signals of dis-improvement in the percentage of all attendees aged 75 years and over at ED who were discharged or admitted within 6 hours since December 2020. The number of inpatient discharges and the number of day cases decreased in May 2021 although this was within the range of variation expected. The data for the number of people on the inpatient and day case active waiting lists in July showed a slight increase followed by a decrease in August and September. Data for 31st August and September 2021 showed that the number of delayed transfers of care were above the upper control limits of the SPC and were therefore higher than expected. There was a slight reduction in the percentage of patients waiting less than 13 weeks following a referral for routine colonoscopy followed by slight increases in August and September. There was a decrease in the number patients completing radical radiotherapy treatment in May

2021, but activity increased in June and July. The average number of patients triaged as urgent presenting to symptomatic breast clinics patients decreased by 20% in May but remained above average. The average number of patients attending rapid access prostate clinics almost remained unchanged. There was a decrease in the average number of patients attending rapid access lung clinics in May 2021 but within the expected range of variation. The upward trend has continued for the average percentage of child health & development assessments completed on time or before 12 months.

The *AAR findings* revealed that the impact of the ICT failure was more profound on acute settings as many of these services relied completely on electronic systems. Areas such as Laboratory, Pharmacy, Radiology or EHR systems which are dependent on ICT suffered significant service disruptions. Various manual workarounds were implemented which meant that it was difficult to ensure that all relevant information was recorded accurately and consistently on paper. As all HSE areas were affected by the ICT outage including those at National level, it was not surprising that some staff perceived that there was scope for improving communication from national level to healthcare teams and the public. Other staff reported that they have lost confidence in the information technology systems. AARs also revealed that the health system was not prepared to deal with a system wide outage of this magnitude and duration. The back loading of information and data that was recorded on paper is a time-consuming process. It is likely that some patient safety impacts of the cyber-attack will remain after all systems have been restored.

The *focus group findings* supported the findings from the other work packages. The participants in acute and maternity services were completely reliant on ICT systems for care delivery and were more severely impacted as compared to community care. The cyber-attack's duration was unprecedented, and the backup systems available were not designed for such events. All services experienced delays and disruptions in service provision. Radiology, radiotherapy, laboratory, and maternity lost access to nearly all systems. Staff developed and implemented innovative manual workarounds to maintain patient care. However, staff are under high levels of stress as they had to deal with challenges of the COVID-19 pandemic and the cyber-attack resulting in a negative impact on staff wellbeing and mental health. Participants identified several gaps in top-down communication during the cyber-attack. Weaknesses in the IT infrastructure in the health system and lack of suitable ICT support structures also became evident during the cyber-attack. The participants stressed that the services are still in the process of recovering from the cyber-attack and there are many on-going challenges to overcome. Concern was expressed regarding the impact on patient safety in the future due to potential missing patient data and information from the time of the cyber-attack.

5. Discussion

Clinical services in Ireland have become increasingly dependent on technology with latent risks accumulating over the course of time. The literature reviewed as part of this report supports the view that services with the highest levels of digitisation are most severely impacted by ICT downtime events. This was observed in the findings of this study particularly in acute and maternity services which were highly reliant on ICT and were completely immobilised. Some staff in these services had only been trained in an environment that was completely reliant on an electronic system and switching to paper-based forms proved to be a challenge. Community healthcare organisations which were less integrated into the HSE network were less impacted, providing further proof that the more a service was digitised, the higher was the impact. The findings of this study indicate that the impact of the cyber-attack was exacerbated by the depletion of local IT support alongside the development of central IT services. Many of the impacts on Patient Safety identified in this study are consistent with the experience of other healthcare organisations that have been affected by significant disruptions due to ICT technology failures.

An important theme in the findings of this study is the impact of the cyber-attack on staff. The cyber-attack had an immediate impact on staff. The risk to patients was mitigated by staff action and there is no evidence of harm to patients in the immediate time period of the attack. However harm may become evident over time though it will be difficult to separate this from the effect of the pandemic. Trust in technology has been impacted which may hinder the adoption of new clinical IT systems in the future. Work needs to focus on assuring that that learning from this cyber-attack has resulted in more security for clinical systems in the Irish healthcare setting. Another important finding in relation to impact on staff was the sense of fear, anxiety and stress experienced by staff. The effect on staff stress must be viewed through the context of the COVID pandemic with the cyber-attack exacerbating an already uncertain and stressful work environment. Our findings indicate that the impact on staff stress may have been more severe than COVID which was further amplified due to a lack of public awareness about the impact and duration of the cyber-attack. This was common across all care areas and needs immediate consideration at a national level. A high level of teamwork, coordination cooperation was observed between GPs, private healthcare providers and testing facilities, within and across teams and disciplines. This was achieved through the flexibility, resilience, and adaptability of staff in the face of uncertain situations and needs to be further recognised and appreciated at HSE management level.

The development of local and national contingency plans should take into account the finding about the limited amount of information recorded on backup systems which were designed with downtimes or shorter duration. Services had no access to medical histories, notes or diagnostic findings, appointment schedules and had to sometimes rely on service user's or staffs' ability to recall information posing a large risk to patient safety. Therefore, the need to evaluate the usefulness of existing back-ups and plan for back-ups that would remain effective, even in longer term downtime events is a key learning point of this report.

Experienced staff assumed leadership roles during the attack and offered reassurance and guidance to colleagues who had no experience using paper-based records. The knowledge and experience of these staff members ensured that risks to patient safety were minimised and provided invaluable insights that must be captured and sustained. However, the findings highlight the risk posed by paper-based forms that were used during the cyber-attack being structured differently from electronic forms as critical information may not have been captured in all cases. This resulted in a knock-on effect that saw the incomplete reconciliation of data once systems were restored. There is a clear need for alignment between paper-based forms and electronic forms at a national level. In addition, study participants indicated that missing data may never be recovered which may lead to risks emerging in the future. The impact of the irretrievable loss of clinical information will not be evident for some time. The long-term impact of cyber-attacks is not well documented in the literature suggesting further research is warranted. .

A common theme was the lack of training and preparedness among staff in dealing with cyber-attacks of this duration and magnitude. Teams reflected on their experience during the cyber-attack and observed that they neither fully anticipated nor were fully prepared to deal with an ICT downtime event of this magnitude. Previous studies have suggested that cyber security awareness and education programmes may prove useful in providing useful skills for healthcare staff (29). This was also evident in the findings as staff considered practical training and preparation for dealing with ICT downtime events as an essential and regular activity in future.

Previous studies have highlighted the need for healthcare professionals to understand the relationship between information technology and patient safety and the knowledge to keep systems and health data secure (29). The findings of this study indicate that the cyber-attack has not only led to recognition among Irish healthcare professionals about the critical role of healthcare ICT systems for patient safety but also sparked discussions around how the health system could be better prepared and proactive in future. While the devastating impact of the cyber-attack on healthcare services is uncontested, it has also presented an opportunity to build on the increased awareness of staff about the importance of cyber security to build systems, processes, and people.

The literature highlights the importance of a coordinated and streamlined effort while responding to cyber-attacks (16). This was also evident from the findings of the study as some staff described unclear governance and a segmented approach as possible barriers to an effective response. Communication is a critical factor in the response to any ICT downtime or cyber-attack (30).

Effective communication enables multi-disciplinary teams to safely transition back from downtime workarounds to routine ICT based systems with no harm to patients (13). The findings of this study suggest there may be an opportunity to improve layering of communication messages to healthcare teams and the public. However, it is important to note that the cyber-attack affected the entire HSE including those working at National level. The findings of this study highlighted that major clinical areas need to develop their governance structures and develop plans and contingencies, develop national networks of communication so that they can share learning and plan. The successful mitigations developed and learning of individual departments and hospitals are an invaluable resource and should be shared with colleagues nationally.

5.1. Key learning

The key learning below have been informed by both international literature and the findings of the study. During a 3-hour workshop, the study team identified and categorised the key learning into what worked well and what could be improved at local (organisation and hospital group) and national level. Following a huge effort, the majority of services have been able to clear most of their information and data entry backlogs. It is essential to acknowledge and further strengthen the strategies and mitigations that worked well during this time.

Table 5.1: What worked well?

Working across traditional boundaries	• The cyber-attack resulted in the flattening of the hierarchy with shared decision making at local levels leading to an empowered frontline. • Staff developed an understanding of the role and responsibilities of various departments/teams (for example clinical staff recognising the important role of clerical and administrative staff). • Services with national clinical structures/organisations in place had better information sharing, ability to raise risks, and share learning- e.g. AMRIC • The importance of having good relationships with other staff, departments, vendors, and service-users was identified as a key learning. • The high degree/level of cooperation between HSE and private providers (GPs, private hospitals, and testing facilities) ensured the impact on patient care was minimised.
Staff skill development	• The participants were able to develop new skills in the areas of IT; computers and using different equipment (for example fax machines).

• Staff displayed resilience in adapting to the environment and there was great teamwork and coordination at local levels.

Table 5.2: What could be improved?

Theme	Local Level	National Level
Contingency planning and preparedness for ICT downtimes	• The importance of each local service/ department developing contingency plans. Evaluation, review, and reflection on the delivery of patient care, services and mitigations developed during the cyber-attack, noting what worked well and what didn't will help inform these contingency plans. • The cyber-attack has highlighted the need to ensure paper-based documentation is in place that reflects the digital system to enable staff to adapt quickly and safely. • It is important that staff are aware of and trained on contingency plans for example the use of paper-based versions of forms. Stimulation exercises and desktop learning may be helpfully here. • Having a list of local ICT systems and the location of backups is valuable for individual services and departments. • The promotion of cyber security awareness among staff will enhance adherence to security policies	• Clinical preparedness emergency plans which are tested regularly are invaluable for such system downtimes • National oversight for local level contingency plans could ensure organisation and service level needs are not overlooked • National governance and communication structures are important aspects of contingency plans • Possible breaches of data and incidents that may arise in future due to the cyber-attack merit close consideration and planning
Improved communication	• The importance of local level managers ensuring their staff is aware of escalation procedures. • Contingency plans would be enhanced by the inclusion of methods of communicating with staff. • Social media may be a useful method to communicate clearly with off-site service users and patients in emergency situations.	• Communication plays a vital role in informing healthcare staff, the public, third parties and regulators to improve awareness of service disruptions, their duration, and on-going issues. • Social media platforms are effective and rapid methods to communicate with the public during an emergency.
Addressing staff concerns	• Where possible, protected staff time should be provided for clearing data backlogs • Consideration should be given to how best to plan to support and facilitate staff to seek	• Staff and public confidence and trust in ICT systems have been negatively impacted during the cyber-attack

help for their mental and physical well-being	• Staff across all aspects of the health system responded with flexibility, commitment, and dedication during the cyber-attack and deserve huge admiration for their work. • Staff fatigue and possible metal health issues have been compounded by the cyber-attack following the stress of working through a pandemic. This may impact sick leave and staff retention.

5.2. Concluding remarks

The Conti cyber-attack on the Health Service Executive (HSE) in May 2021 had a significant impact on many HSE services. This study focused on the clinical and patient safety impact of the cyber-attack with the objective of completing a comprehensive analysis of the impact of the cyber-attack on patient safety; the impact on patient safety of the loss of key systems, the mitigations put in place and to capture key learnings. A mixed methods analysis was applied using a literature review and a mix of qualitative and quantitative methods organised into 3 work packages: 1. Content analysis of risk register and incident analysis, 2. Quantitative analysis of routinely available national data, and 3. Qualitative analysis of after-action review documents and qualitative focus groups. The focus on the clinical impact is a limitation of this study, as the methodology employed focused on capturing the experiences of clinicians and those working in healthcare settings. The findings must therefore be understood in this context with learning aimed at supporting clinical services and patient safety and therefore it may be prudent to consider the HSE management and IT feedback in its translation.

It is important to acknowledge that hindsight bias may have helped identify accumulating and invisible risks in clinical services in this study. However, a striking feature of the analysis is the consistency and alignment of findings across all methods employed. Many examples of how patient safety was maintained despite the disruption to ICT systems were described both during the focus groups and during after action reviews. Staff should be commended for their innovation and commitment to providing safe patient care. The metrics analysed showed that the impact on service users and families was less than that associated with the Covid-19 pandemic response and can be attributed to the significant efforts of staff to maintain services. While no incidents directly attributed to the cyber-attack were identified in our analysis, this will be reviewed to identify if any patient safety incidents attributable to the cyber-attack emerge in the future.

The impact of the cyber-attack on staff was significant and, in some cases, is on-going as of November 2021. The contribution that well designed clinical ICT systems make to Patient Safety was clear across several datasets. There was broad agreement that those services where significant clinical ICT systems have been implemented were impacted most severely. Services with little dependence on ICT systems commented that the impact was comparatively low. Within these conversations, a risk was identified in relation to the confidence level in clinical ICT systems. Some staff felt that future roll out of national ICT systems may meet resistance given the level of disruption experienced by services with significant ICT system implementation. It is a key learning of this report that patient safety strategies are significantly strengthened through the use of ICT systems. Informing contingency planning for possible future ICT outages is therefore a key aim of this report and will help to ensure that patient safety remains central to the delivery of care. It is now vital that plans are developed to consider and minimise the patient safety risks that may emerge in the future due to the impact of the cyber-attack at department, service, and national level.

References

1. Institute of Medicine Committee on Data Standards for Patient S. Patient Safety: Achieving a New Standard for Care. In: Aspden P, Corrigan JM, Wolcott J, Erickson SM, editors. Patient Safety: Achieving a New Standard for Care. Washington (DC): National Academies Press (US)

Copyright 2004 by the National Academy of Sciences. All rights reserved.; 2004.

2. Emanuel L, Berwick D, Conway J, Combes J, Hatlie M, Leape L, et al. What exactly is patient safety? Journal of Medical Regulation. 2009;95(1):13-24.

3. Institute of medicine. Crossing the Quality Chasm: A New Health System for the 21st Century. Washington DC: Institute of medicine; 2001.

4. Health Service Executive Ireland. Patient Safety Strategy 2019-2024. Dublin, Ireland: Health Service Executive Ireland; 2019. Contract No.: 978-1-78602-127-4.

5. Ross J. Cyber security: A Real Threat to Patient Safety. Journal of PeriAnesthesia Nursing. 2017;32(4):370-2.

6. Argaw ST, Bempong N-E, Eshaya-Chauvin B, Flahault A. The state of research on cyber-attacks against hospitals and available best practice recommendations: a scoping review. BMC Medical Informatics and Decision Making. 2019;19(1):10.

7. Ghafur S, Kristensen S, Honeyford K, Martin G, Darzi A, Aylin P. A retrospective impact analysis of the WannaCry cyber-attack on the NHS. npj Digital Medicine. 2019;2(1):98.

8. Muthuppalaniappan MLLB, Stevenson K. Healthcare cyber-attacks and the COVID-19 pandemic: an urgent threat to global health. International Journal for Quality in Healthcare. 2021;33(1).

9. Pranggono B, Arabo A. COVID-19 pandemic cyber security issues. Internet Technology Letters. 2021;4(2):e247.

10. Martin G, Kinross J, Hankin C. Effective cyber security is fundamental to patient safety. BMJ. 2017;357:j2375.

11. Barad M. Linking Cyber Security Improvement Actions in Healthcare Systems to Their Strategic Improvement Needs. Procedia Manufacturing. 2019;39:279-86.

12. Coffey P, Postal S, Houston S, McKeeby J. Lessons Learned from an Electronic Health Record Downtime. Perspectives in Health Information Management. 2016(Summer).

13. Dave K, Boorman RJ, Walker RM. Management of a critical downtime event involving integrated electronic health record. Collegian. 2020;27(5):542-52.

14. Scantlebury A, Sheard L, Fedell C, Wright J. What are the implications for patient safety and experience of a major healthcare IT breakdown? A qualitative study. DIGITAL HEALTH. 2021;7:20552076211010033.

15. Wang Y, Coiera E, Gallego B, Concha OP, Ong MS, Tsafnat G, et al. Measuring the effects of computer downtime on hospital pathology processes. J Biomed Inform. 2016;59:308-15.

16. Chen P-H, Bodak R, Gandhi NS. Ransomware Recovery and Imaging Operations: Lessons Learned and Planning Considerations. Journal of digital imaging. 2021;34(3):731-40.

17. Larsen E, Hoffman D, Rivera C, Kleiner BM, Wernz C, Ratwani RM. Continuing Patient Care during Electronic Health Record Downtime. Applied clinical informatics. 2019;10(3):495-504.

18. Magrabi F, Liaw ST, Arachi D, Runciman W, Coiera E, Kidd MR. Identifying patient safety problems associated with information technology in general practice: an analysis of incident reports. BMJ Qual Saf. 2016;25(11):870-80.

19. Martin G, Ghafur S, Cingolani I, Symons J, King D, Arora S, et al. The effects and preventability of 2627 patient safety incidents related to health information technology failures: a retrospective analysis of 10 years of incident reporting in England and Wales. The Lancet Digital Health. 2019;1(3):e127-e35.

20. Chen JA, Wang Y, Magrabi F, editors. Downtime in Digital Hospitals: An Analysis of Patterns and Causes Over 33 Months. HIC; 2017.

21. Klokman VW, Barten DG, Peters NALR, Versteegen MGJ, Wijnands JJJ, van Osch FHM, et al. A scoping review of internal hospital crises and disasters in the Netherlands, 2000–2020. PLOS ONE. 2021;16(4):e0250551.

22. Health Service Executive Ireland. Incident Management Framework. Health Service Executive Ireland; 2020. Report No.: 978-1-78602-161-8.

23. Mohammad S. NRC Word-Emotion Association Lexicon. Canada2010.

24. Mohammad SM, Turney PD. Crowdsourcing a word–emotion association lexicon. Computational intelligence. 2013;29(3):436-65.

25. R Core Team. R: A language and environment for statistical computing. Vienna, Austria: R Foundation for Statistical Computing; 2021.

26. Savoia E, Agboola F, Biddinger PD. Use of After Action Reports (AARs) to Promote Organizational and Systems Learning in Emergency Preparedness. International Journal of Environmental Research and Public Health. 2012;9(8).

27. Braun V, Clarke V. Using thematic analysis in psychology. Qualitative Research in Psychology. 2006;Volume 3, 2006(2).

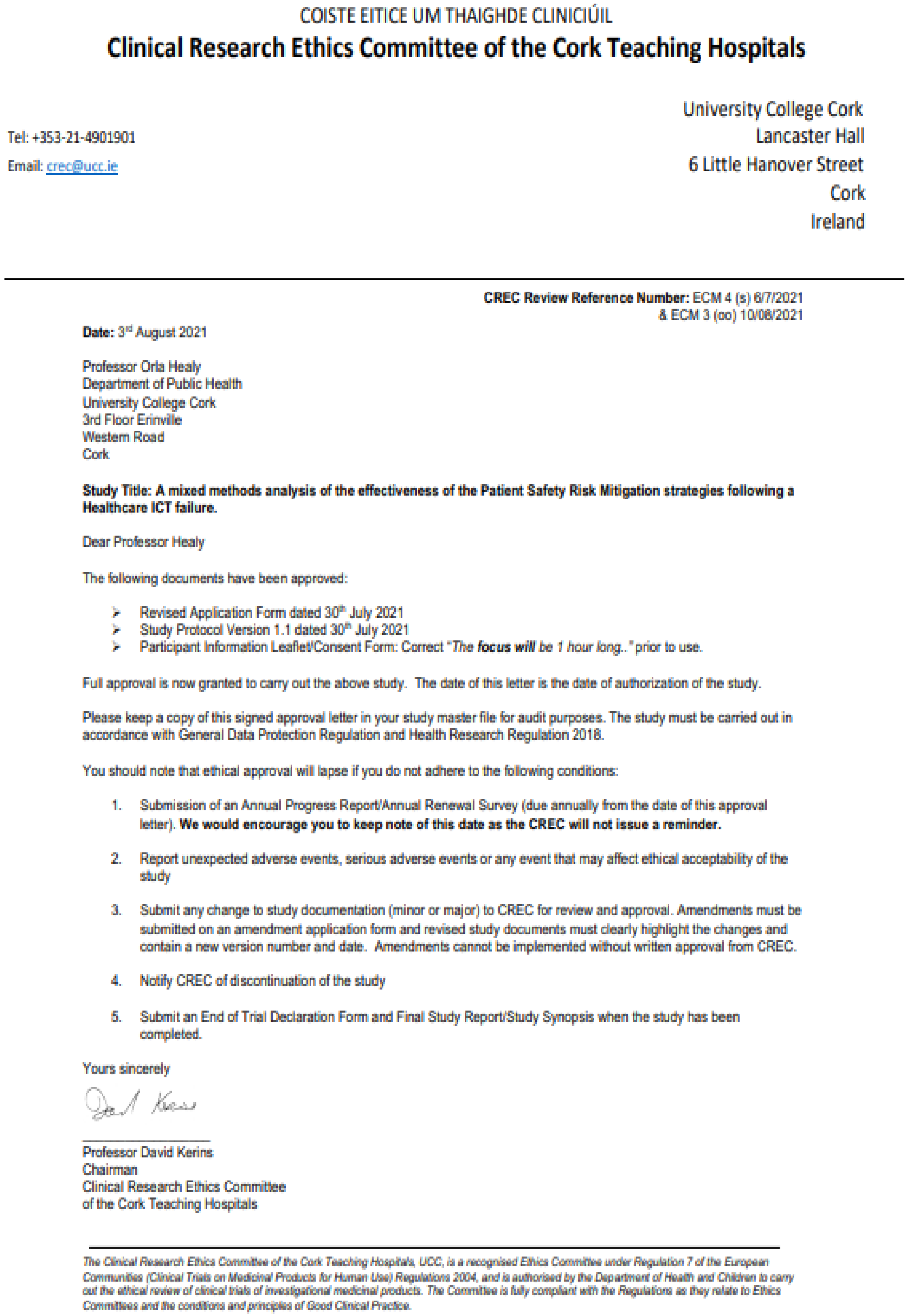
28. QSR International Pty Ltd. NVivo qualitative data analysis software. Version 12 ed2018.

29. O'Brien N, Ghafur S, Durkin M. Cyber security in health is an urgent patient safety concern: We can learn from existing patient safety improvement strategies to address it. Journal of Patient Safety and Risk Management. 2021;26(1):5-10.

30. Kashiwagi DT, Sexton MD, Souchet Graves CE, Johnson JM, Callies BI, Jr., Yu RC, et al. All CLEAR? Preparing for IT Downtime. Am J Med Qual. 2017;32(5):547-51.

Appendices

Appendix File 1: Ethics approval



COISTE EITICE UM THAIGHDE CLINICIÚIL

Clinical Research Ethics Committee of the Cork Teaching Hospitals

University College Cork
Lancaster Hall
6 Little Hanover Street
Cork
Ireland

Tel: +353-21-4901901
Email: crec@ucc.ie

CREC Review Reference Number: ECM 4 (s) 6/7/2021
& ECM 3 (oo) 10/08/2021

Date: 3rd August 2021

Professor Orla Healy
Department of Public Health
University College Cork
3rd Floor Erinville
Western Road
Cork

Study Title: A mixed methods analysis of the effectiveness of the Patient Safety Risk Mitigation strategies following a Healthcare ICT failure.

Dear Professor Healy

The following documents have been approved:

- Revised Application Form dated 30th July 2021
- Study Protocol Version 1.1 dated 30th July 2021
- Participant Information Leaflet/Consent Form: Correct "*The **focus will** be 1 hour long..*" prior to use.

Full approval is now granted to carry out the above study. The date of this letter is the date of authorization of the study.

Please keep a copy of this signed approval letter in your study master file for audit purposes. The study must be carried out in accordance with General Data Protection Regulation and Health Research Regulation 2018.

You should note that ethical approval will lapse if you do not adhere to the following conditions:

1. Submission of an Annual Progress Report/Annual Renewal Survey (due annually from the date of this approval letter). **We would encourage you to keep note of this date as the CREC will not issue a reminder.**

2. Report unexpected adverse events, serious adverse events or any event that may affect ethical acceptability of the study

3. Submit any change to study documentation (minor or major) to CREC for review and approval. Amendments must be submitted on an amendment application form and revised study documents must clearly highlight the changes and contain a new version number and date. Amendments cannot be implemented without written approval from CREC.

4. Notify CREC of discontinuation of the study

5. Submit an End of Trial Declaration Form and Final Study Report/Study Synopsis when the study has been completed.

Yours sincerely

Professor David Kerins
Chairman
Clinical Research Ethics Committee
of the Cork Teaching Hospitals

The Clinical Research Ethics Committee of the Cork Teaching Hospitals, UCC, is a recognised Ethics Committee under Regulation 7 of the European Communities (Clinical Trials on Medicinal Products for Human Use) Regulations 2004, and is authorised by the Department of Health and Children to carry out the ethical review of clinical trials of investigational medicinal products. The Committee is fully compliant with the Regulations as they relate to Ethics Committees and the conditions and principles of Good Clinical Practice.

Appendix File 2: Study information sheet

Seirbhís Sláinte
Níos Fearr
á Forbairt

Building a
Better Health
Service

PARTICIPANT INFORMATION SHEET

Study Title: A mixed methods analysis of the effectiveness of the Patient Safety Risk Mitigation strategies following a Healthcare Information Communication Technology failure

Principal Investigators: Professor Orla Healy[1]

Researchers: Dr Gemma Moore[2,] Ms. Zuneera Khurshid[3]

You are kindly invited to take part in this research to explore the risk mitigation measures and contingencies required to safely deliver patient services and maintain health and social care services in the event of an either partial or complete Information Communication Technology outage and to understand what worked well and where is there scope for improvement. The research is being conducted by the Quality and Patient Safety Division of the HSE. Before you make your participation decision, we would like you to understand why the research is being conducted and what it would involve for you. Please take your time to read this information. You can ask for any clarification or further information by contacting us using the details at the end of this information sheet.

Information About This Study

What is this research and why is the research being done?

In May 2021, HSE Information Communication Technology systems were the subject of a ransomware attack that resulted in widespread outages of critical Information Communication Technology systems. The objective of this study is to conduct a timely review of the mitigations and contingencies adopted in the Irish health system to minimize the impact on patient safety. In addition, the study will focus on the learning regarding what worked well to inform future planning for further Information Communication Technology outages. We are now seeking your consent to take part in a voluntary interview or focus group for the study. Team members will collectively decide whether they wish to participate

[1] HSE National Clinical Lead for Patient Safety and Adjunct Clinical Professor in the Department of Epidemiology and Public Health in UCC
[2] Qualitative Data Lead, Evidence for Improvement, National Quality Improvement Team, HSE
[3] PhD Candidate, University College Dublin

in individual interviews or one focus group for the entire team. This interview will take approximately 30-40 minutes and will be conducted over the phone or as an online meeting depending on your preference. The focus group will be 1 hour long and conducted using an online meeting platform. Interviews and focus groups will be audio recorded, and pseudonyms will be used in the research reports. You have the right to withdraw from participation in the interview at any point.

Why have I been asked to take part?

You have been invited to take part in the research because we want to explore the experience of staff working in acute and community settings impacted by the cyber-attack.

Do I have to take part?

Participation in this study is entirely voluntary. It is up to you to decide whether you would like to take part or not. If you agree to take part, we will ask you to sign a consent form. You are free to refuse to take part, or to withdraw at any point, without giving a reason and without any adverse effects as a finding.

What will happen if I agree to take part?

If you agree to take part, the research team will ask you to sign a consent form. By opting into the study, you will be sharing your experiences of what mitigations were successful or unsuccessful from a patient safety perspective and the key learning to minimise the impact on patient safety in the case of an IT outage in the future. You are also agreeing to be contacted by the research team by email/ phone (based on your personal contact preference) about your engagement in the research.

Will I receive any expenses or payments?

We will not provide any payments or cover any expenses for your participation in this research.

What are the possible risks of taking part?

We do not envisage any harm to participants due to their participation in the research. If you decide to take part in the study, you are free to withdraw any time without question or reason. Should any information come to light during the research that would suggest malpractice or misconduct or indicate that any individual was in danger of harm; the researchers are obliged to report this to the appropriate personnel.

In the unlikely event during data collection and analysis that the researchers interpret a situation as presenting an on-going serious safety concern in respect of service provision and/or posing a clinical risk, the researcher will, where possible, bring this to the attention of the participant who highlighted the issue and ask them to submit the concern or report the incident through the appropriate channels. In addition, the researcher will include reference to the said concern in the research findings report which will be reviewed by your unit prior to circulation to the hospital management team. The report findings will be in aggregate form and all respondents and data will be anonymised.

If the nature of the concern were one that could in the view of the researcher cause serious direct and severe harm to patients, the researcher would be obliged to report this to the unit manager at the earliest opportunity. Respondents would be anonymised in the said report.

What are the possible benefits of taking part?

Your participation in this research will enable the Irish health system to learn from staff experiences and apply this learning to inform future healthcare policy, planning and delivery. The research will also contribute towards quality and patient safety research on issues of national priority with the potential to make a real difference to the Irish health service. It will also highlight the extraordinary work being undertaken Irish the healthcare staff to ensure service continuity during this cyber-attack.

What will happen if I change my mind about taking part?

If you agree to take part but later decide that you wish to withdraw, please contact a member of the research team using the contact details at the end of this leaflet. If you withdraw your consent during the study, you will not have to continue to take part in the study.

Will my taking part in the study be kept confidential?

Your name will not appear in reports, publications or presentations arising from the research. In accordance with HSE’s policy on data protection and storage, the paper versions of consent forms will be anonymised (your name and any identifying details will not be included) and will be kept in a locked filing cabinet in the HSE. These will only be available to members of the research team. Interviews will be transcribed and securely stored on password protected computers. Following transcription, taped recordings will be destroyed. The anonymised transcripts will be held by the HSE for 2 years then securely destroyed.

What will happen to the findings of the study?

The findings of this study will inform future planning to minimize the impact on patient safety of Information Communication Technology outages at local and national level. We intend to publish the findings in reports, scientific journals and to present at national and international conferences.

Who is organising and funding the research?

The research is being conducted by the Quality and Patient Safety Division of the HSE.

Who has reviewed the study?

This study has received favourable ethical opinion by Clinical Research Ethics Committee of the Cork Teaching Hospitals.

How will I find out what happens with this project?

If you would like to receive a summary of the findings, you can notify the researcher that you would like to be contacted for this purpose.

What happens next?

If you are happy to proceed, we will explain the study and answer any questions you may have.

How to contact us?

If you have any concerns about the study, or would like more information, please contact:

Dr. Gemma Moore PhD

Email: gemma.moore2@hse.ie

Thank you for taking the time to read this information

Appendix 3: Interview and focus group topic guide

Introductory questions

1. Could I ask you **introduce** yourself and describe your **role and responsibilities** in your team?

Impact of Cyber-attack

2. I am interested in understanding the **impact** of the cyber-attack on how you work. What IT systems, software, and networked devices that you use were impacted by the cyber-attack?
    - How did not having access to these systems impact the services your team provides?
        - ➔ Probe further on impact on patient care, delayed procedures etc.
3. Was there effective communication to front line staff during the attack?
    - Did you feel you could effectively communicate and escalate risks and issues to clinical and executive management?
    - Were the risks you reported acted on?
        - ➔ Probe on whether they got feedback and assurance on the risks they reported

Mitigations

4. Could you describe the **mitigations** and workarounds that were developed to ensure continuity of services
    - How were these mitigations developed (e.g. team huddles, revision over time)

5. How did you **prioritise** the services you delivered?
    - Were there any trade-offs involved or reduction of normal practices?

6. Which of the mitigations developed worked well and which didn’t?
    - Will you retain any of mitigations in your normal routine or work practices going forward?
    - Are these mitigations being retained service wide or just within your team?
    - Who were the decision makers behind retaining the mitigations (Senior management, Local management, team?)
        - ➔ Probe on potential risks this might involve

7. Has the team and/or organisation discussed **strategies and contingency plans** for possible **future outages**?

- ◦ Which mitigations do you plan on putting in place?

Quality and Safety

8. In your opinion, was there an **impact on the quality and safety of patient care** during this time?

- ◦ Were different issues and risks more significant in certain stages of the cyber-attack? e.g. In the initial few days, while implementing workarounds or while returning to normalcy?
    - ➔ Probe on whether they are aware of any lost data during the down time
    - ➔ Probe on impact on backlogs, wait times, communications between departments, delays,

9. Are you aware of any **actual incidents** or errors that occurred during this time that can be attributed to the cyber-attack?

- ◦ Were any of these serious incidents or errors that caused harm?

10. Did you think the cyber-attack influenced the levels of **stress and fatigue** among your team?

Summary

11. What is the current status and expectations about resumption of full services?

- ◦ Probe on whether they are aware of any lost data during the down time

12. What is the **key learning** for the team from this experience?

Appendix 4a: Interview consent form

Seirbhís Sláinte
Níos Fearr
á Forbairt

Building a
Better Health
Service

PARTICIPANT CONSENT FORM

Study Title: A mixed methods analysis of the effectiveness of the Patient Safety Risk Mitigation strategies following an Information Communication Technology failure

Principal Investigators: Professor Orla Healy[1]

Researchers: Dr Gemma Moore[2], Ms. Zuneera Khurshid[3]

Participant Number:

Please tick each

1. I have read the information sheet and understand that I will be involved in this research to explore the effectiveness of the Patient Safety Risk Mitigation strategies following a Healthcare Information Communication Technology failure	
2. I understand that my participation in this study is voluntary and that I am free to withdraw my participation at any time without giving a reason.	
3. I understand that I will be taking part in a 30-40 minute or interview with a member of the research team, but that this is voluntary, and I can decline to take part if I wish. If I choose to take part, I know I can withdraw at any point up to or during the interview and can receive a copy of my transcript for my review after the interview.	
4. I understand that all data collected during the study will remain confidential, and I consent to my responses and personal information being stored in password protected and encrypted computers.	
5. I understand that if any disclosures are made that would indicate malpractice or misconduct at any point during the study or suggest that any individual was in danger of harm, this information will be disclosed to the appropriate personnel and the researcher would be obliged to report this to the unit manager at the earliest opportunity.	
6. My queries have been addressed to my satisfaction by the research team and I consent to take part in this study.	

Name of participant ______________________ Date ______________ Signature ______________

Name of person taking consent ______________________ Date ______________ Signature ______________

[1] HSE National Clinical Lead for Patient Safety and Adjunct Clinical Professor in the Department of Epidemiology and Public Health in UCC

[2] Qualitative Data Lead, Evidence for Improvement, National Quality Improvement Team, HSE

[3] PhD Candidate, University College Dublin

Appendix 4b: Focus group consent form

Seirbhís Sláinte
Níos Fearr
á Forbairt

Building a
Better Health
Service

PARTICIPANT CONSENT FORM

Study Title: A mixed methods analysis of the effectiveness of the Patient Safety Risk Mitigation strategies following an Information Communication Technology failure

Principal Investigators: Professor Orla Healy

[1]

Researchers: Dr Gemma Moore[2,] Ms. Zuneera Khurshid[3]

Participant Number:

Please tick each

1. I have read the information sheet and understand that I will be involved in this research to explore the effectiveness of the Patient Safety Risk Mitigation strategies following a Healthcare Information Communication Technology failure	
2. I understand that my participation in this study is voluntary and that I am free to withdraw my participation at any time without giving a reason.	
3. I understand that I will be taking part in a 1 hour long focus group with a member of the research team, but that this is voluntary, and I can decline to take part if I wish. If I choose to take part, I know I can withdraw at any point up to or during the interview and can receive a copy of my transcript for my review after the interview.	
4. I understand that all data collected during the study will remain confidential, and I consent to my responses and personal information being stored in password protected and encrypted computers.	
5. I understand that if any disclosures are made that would indicate malpractice or misconduct at any point during the study or suggest that any individual was in danger of harm, this information will be disclosed to the appropriate personnel and the researcher would be obliged to report this to the unit manager at the earliest opportunity.	
6. My queries have been addressed to my satisfaction by the research team and I consent to take part in this study.	

________________________ ______________ ________________________

Name of participant Date Signature

________________________ ______________ ________________________

[1] HSE National Clinical Lead for Patient Safety and Adjunct Clinical Professor in the Department of Epidemiology and Public Health in UCC

[2] Qualitative Data Lead, Evidence for Improvement, National Quality Improvement Team, HSE

[3] PhD Candidate, University College Dublin

Name of person taking consent Date Signature

Appendix 5: SCA report

State Claims Agency

Gníomhaireacht Bainistíochta an Chisteáin Náisiúnta
National Treasury Management Agency

An Ghníomhaireacht um Éilimh ar an Stát
State Claims Agency

NIMS

National Incident Management System

SCA Query Reference	Q217256
Query Title	Report on recording of incidents during cyber-attack
Requestor	Dr. Orla Healy, HSE
Date of request	03/08/2021
Report run date	23/08/2021
Reporting period	2019 – 2021 (from 01/01 to 23/08 for each year)

Introduction

Following the cyber-attack on 14 May 2021 access to NIMS was disabled for all health and social careusers as a precaution. A communication was issued by the HSE on 31 May 2021, advising that completed national incident report forms (NIRFs) could be sent to the State Claims Agency for uploading on NIMS.

This report has been prepared in response to a request from the HSE for an analysis of incident reporting on NIMS during the initial and recovery phases of the cyber-attack, and in particular comparison of incident numbers to date for 2021 with previous years.

The information contained within this document was extracted from the National Incident Management System (NIMS) as per the below criteria.

Please note that the data was run on the 23/08/2021 and the SCA are still processing a backlog of incidents on behalf of the HSE i.e. there are just over 1,000 incidents still to enter on NIMS as part of this work. Therefore, the statistics in this document will not reflect the outstanding backlog of incidents yet to be entered by the SCA on behalf of the HSE.

To the 23rd August, the following incidents have been received and entered by SCA:

Summary Statistics	
Total Incidents Received	5741
Total Incidents Entered	4683
% of Incidents Entered	82%

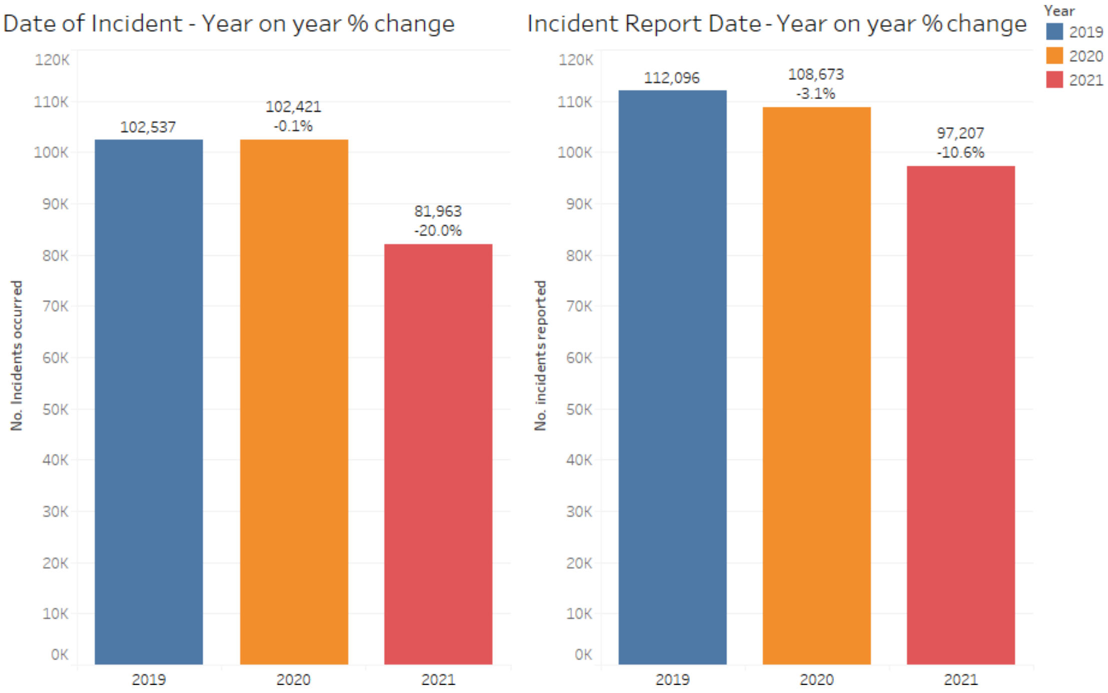
Criteria used

- Location at Level 1: ‘Healthcare’.
- Who/What variable = Incidents relating to Patient and Dangerous Occurrences are included.
- For graphs/tables showing Date of Incident; YTD numbers for 2019, 2020, and 2021 areused.
- For graphs/tables showing Incident Report Date; year to date (YTDD numbers for 2019,2020, 2021 are used.
- This report is correct as of 23/08/2021.

Total year to date reporting year on year for 2019-2021

Date of Incident – The graph shows the number of incidents occurring in 2019 – 2021, from 1st January to 23rd August for each year, and the percentage change year on year. The number of incidents occurred for 2019 and 2020 were consistent, showing only a 0.1% drop. From 2020 to 2021there was 20.0% drop. This can be explained in some part by a lag in the time to report an incidenton NIMS from when it occurred. It would be expected that incidents which have occurred in the laterpart of 2021 can take up to 3 months to be reported after they occur which will increase the total forthis year by a certain amount.

Incident Report Date – The graph shows the number of incidents reported in 2019 – 2021, from 1st January to 23rd August for each year, and the percentage change year on year. The number of incidents reported in 2020 was down 3.1% from 2019, this in part may be due to Covid related issues, although looking at the 'Date of Incident' chart on left the numbers of incidents occurred were almost identical once all incidents were reported on NIMS. From 2020 to 2021 there is over a 10.5% drop in incidents reported.

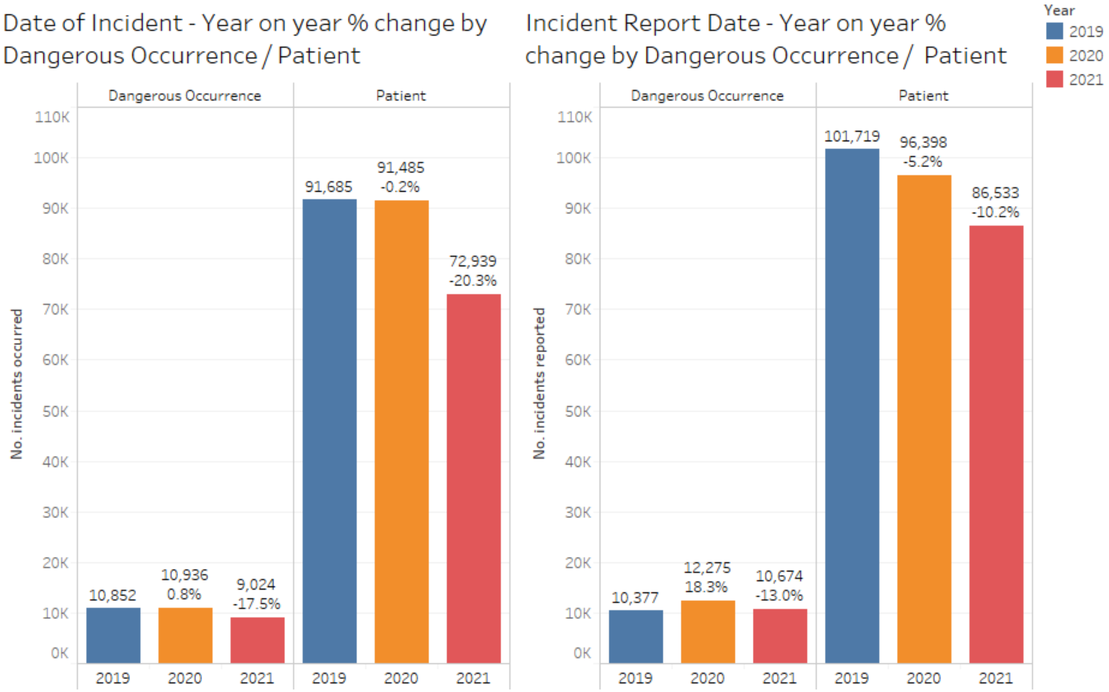


Graph 1: Number of Incidents occurred, and number of incidents reported on NIMS in 2019-2021 to 23rd August eachyear including the percentage change year on year.

Patient and Dangerous Occurrence incidents by Date of Incident andIncident Report date for years 2019-2021 YTD

Date of Incident – The ratio of Patient: Dangerous Occurrences is consistently in the region of approximately 8.4:1 over the 3 years. The reporting numbers for 2019 and 2020 were consistent, even with Covid disruption to services. A slightly larger drop in Patient incidents occurring, comparedto Dangerous Occurrences is observed from 2020 to 2021.

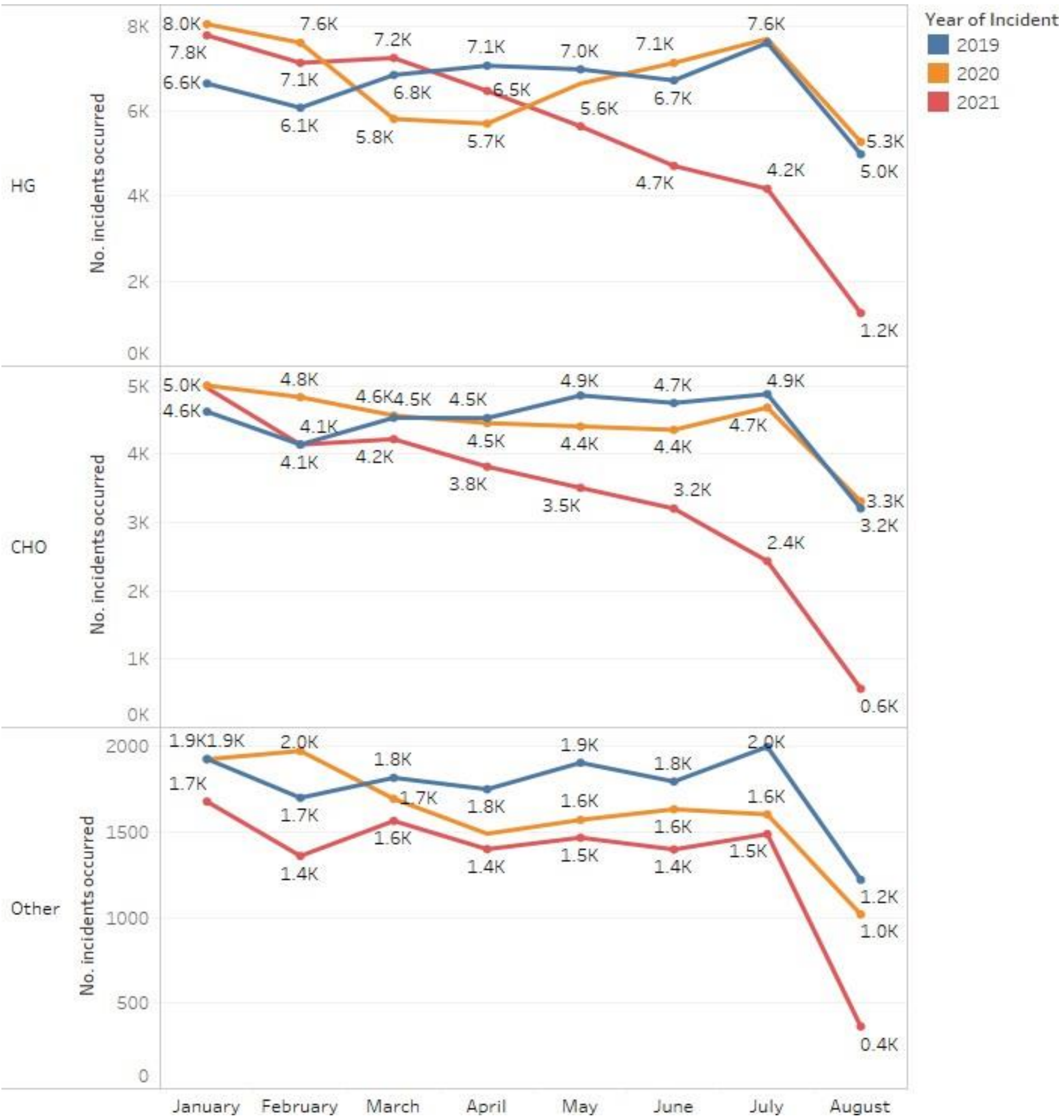
Incident Report Date – The ratio of Patient: Dangerous Occurrence incidents was less consistent when comparing through Incident Report Date. In 2019 the ratio was just under 10:1 compared to approximately 8:1 in 2020 and 2021. It also saw an increase in Dangerous Occurrence incidents reported from 2019 to 2020, and a reduction of Patient incidents in the same time. For 2020, a 5.2% decrease in Patient incidents reported and an 18.3% increase in Dangerous Occurrences may have been expected due to Covid disruption of services. There was a slight reversal in this trend in 2021, with the number of Dangerous Occurrences reported decreased at a greater rate than Patient incidents.



Graph 2: Number of Incidents occurred, and number of incidents reported on NIMS in 2019-2021 to 23rd August eachyear including the percentage change year on year by Dangerous Occurrence / Patient.

Date of Incident year on year for 2019-2021 by month incident occurredand by HG/CHO/Other

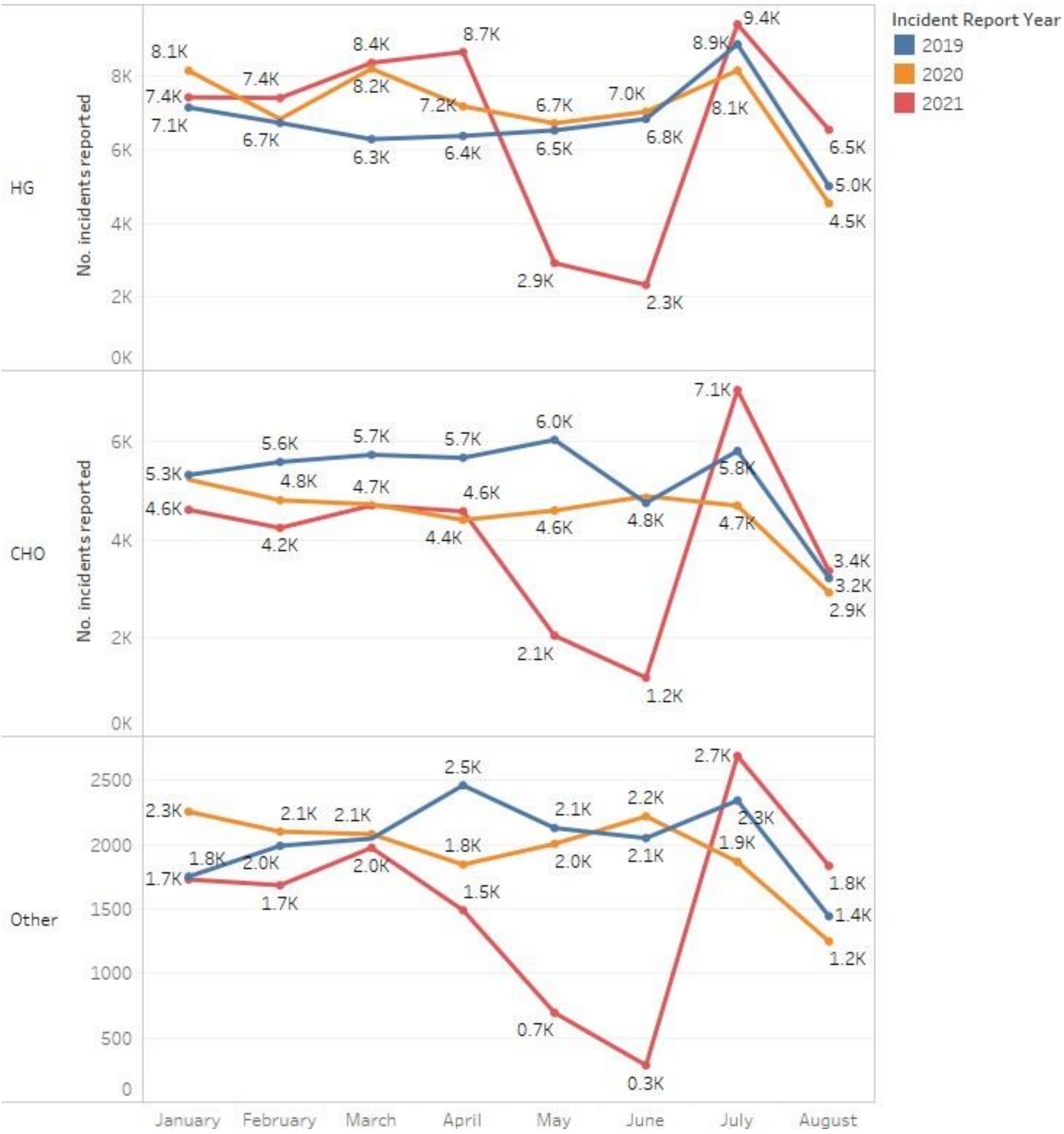
Date of Incident – There is a clear trend of a decrease in Incidents occurring in 2021 from April, with a significant further drop in July/August. 2019 and 2020 have almost identical totals for the year to 23rd August (See Graph 1). The August numbers being the lowest month for 2019 and 2020 is due to only incidents to 23rd August for being included. The largest drop from 2020 to 2021 is seen for CHOsat just 18.1% of the 2020 total being reported, compared to 22.6% for Hospital Groups, and 40.0%for Other locations. This drop will be partially due to the standard reporting delay.



Graph 3: Number of Incidents occurred in 2019-2021 to 23rd August each year, by month.

Note: 'Other' locations includes all locations which are not in a Hospital Group or CHO Area, e.g. National Social Care,National Services and Community.

Incident Report Date – There is a clear drop in incidents reported for May, when the cyber-attack occurred, and June for the year 2021. This is followed by the highest reporting totals of any month inJuly for all locations. The reporting for Hospital Groups in August is up in 2021, by 30.1% on 2019 and44.0% on 2020.For Hospital Groups, 2021 has the highest total of reported incidents in April 2021, compared to 2019 and 2020. While Hospital Groups had higher number of incidents reported year todate in 2020 compared to 2019, it was the opposite for CHOs and Other locations, which were slightly higher in 2019.

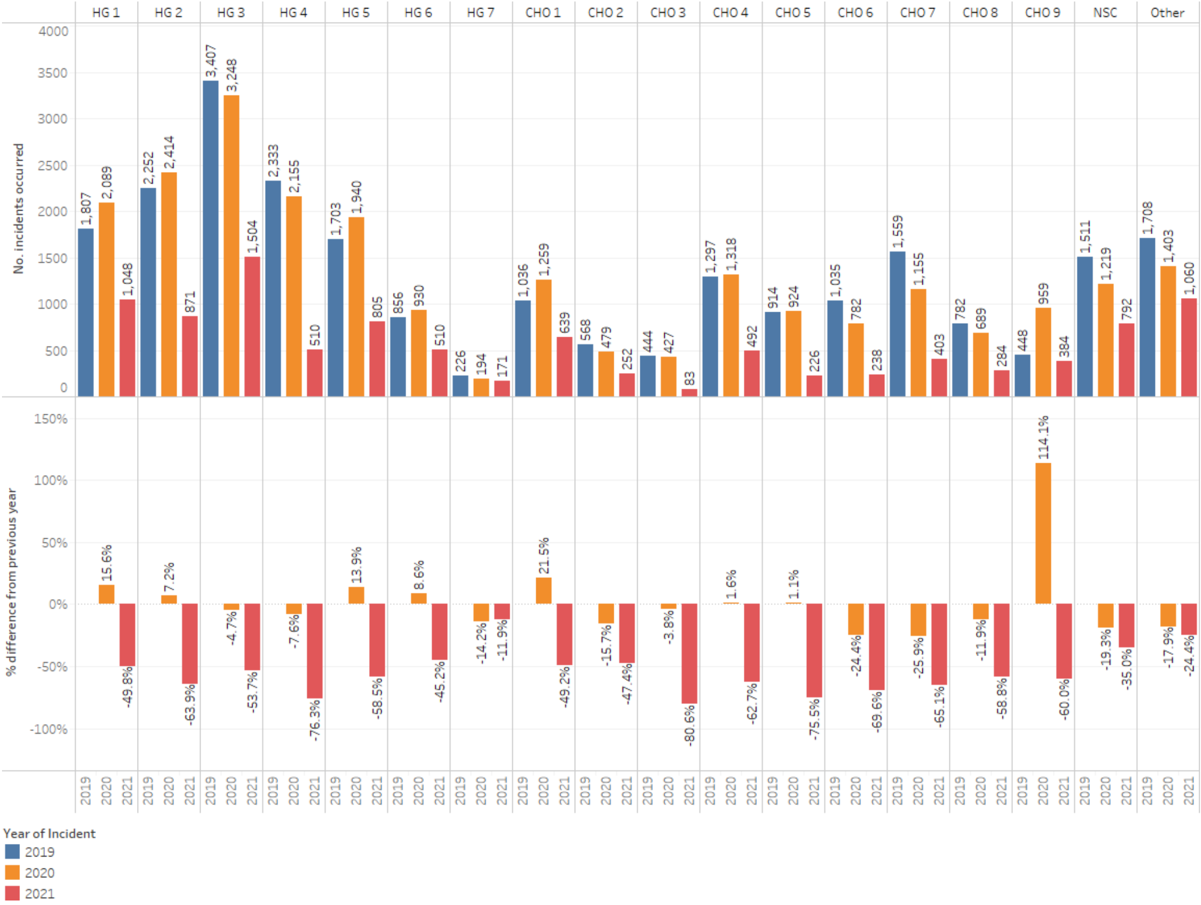


Graph 4: Number of Incidents reported in 2019-2021 to 23rd August each year, by month.

Note: 'Other' locations includes all locations which are not in a Hospital Group or CHO Area, e.g. National Social Care,National Services and Community.

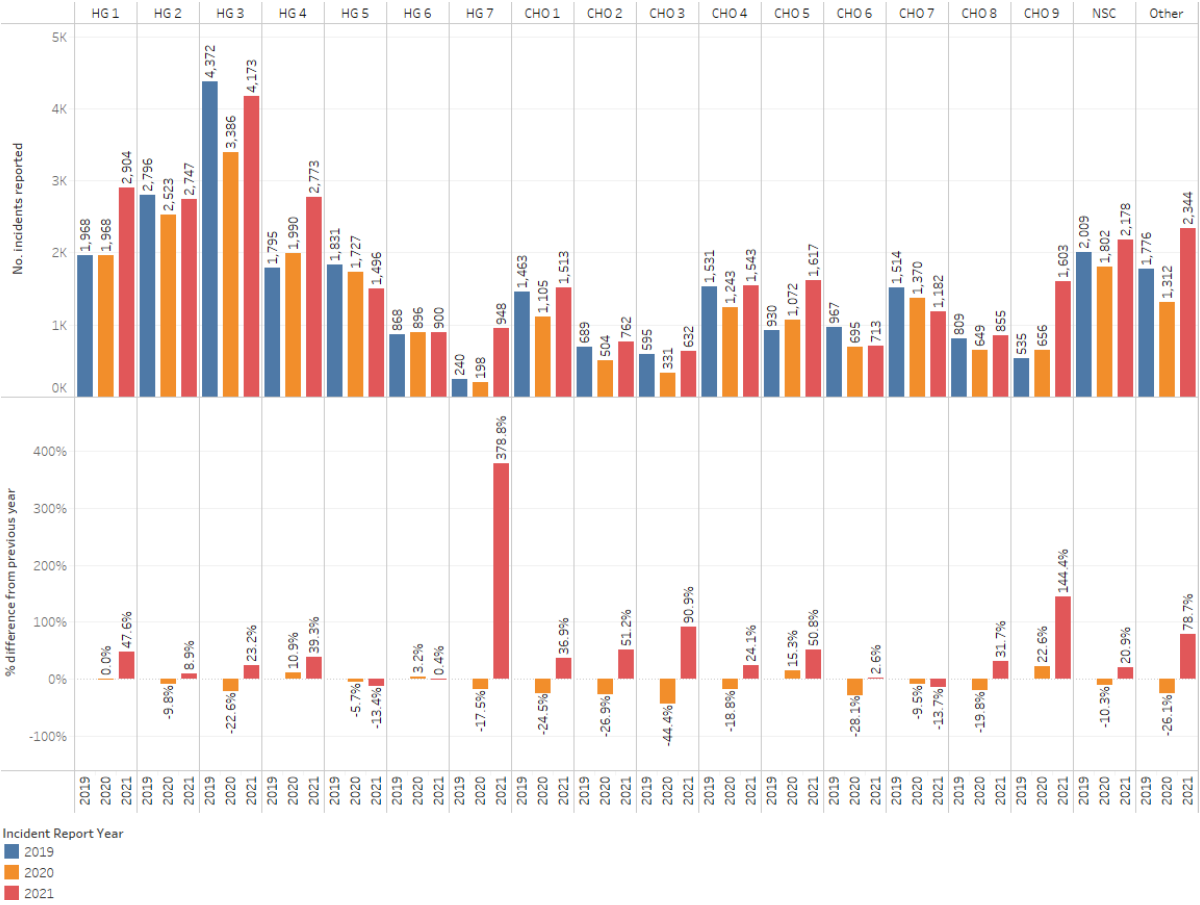
1st July to 23rd August reporting year on year for 2019-2021 by CHO Area, Hospital Group, NSC, and Other HC locations

Date of Incident – Looking at only the incidents occurred from 1st July to 23rd August all locations have a drop off in 2021 compared to the two previous years. In total, Hospital Groups are down 58.2%, CHOs are down 62.5% in 2021 from 2020, and Other locations down 29.4%. The largest drop for a Hospital Group is Group 4 with over a 76.3% drop from 2020 to 2021, with 6 hospitals showinga decrease of over 60%. CHO 3 shows a drop of 80.6%, which is the largest drop for any location.



Graph 5: Year on year incidents occurred by Location for the period 1st July to 31st August for years 2019-2021

Incident Report Date – The number of incidents reported from 1st July to 23rd August 2021 increased for Hospital Groups (up 25.6% on 2020), CHOs (up 36.7% on 2020), and Other locations (up 45.2% on2020). Hospital Group 7 is an outlier due to CHI at Crumlin reporting 570 incidents in 2021 comparedto 58 in 2020. The largest increase in CHOs is CHO 9 which is mainly due to St. Michaels House Ballymun reporting 1,155 incidents in 2021 compared to 365 in 2020.



Graph 6: Year on year incidents reported by Location for the period of 1st July to 23rd August for years 2019-2021

Hospitals showing a drop in incidents reported for 1st July to 23rd Augustyear on year from 2020 to 2021

Hospitals - Sixteen hospitals within the Hospital Groups have shown a decrease in reporting from 1st July to 23rd August in 2021 compared to the same period in 2020. Royal Victoria Eye & Ear Hospital and St. Luke's Radiation Oncology Network have not yet reported any incidents while Midlands Regional Hospital, Portlaoise and St. Columcille's Hospital are down over 80%.

Hospital	Hospital Group	% Difference from previous year			Number of Incidents reported		
		2019	2020	2021	2019	2020	2021
Royal Victoria Eye & Ear Hospital	HG 3	n/a	-76.5%	**-100.0%**	17	4	0
St. Luke's Radiation Oncology Network	HG 2	n/a	606.7%	**-100.0%**	15	106	0
Midland Regional Hospital, Portlaoise	HG 2	n/a	-23.1%	**-85.9%**	333	256	36
St. Columcille's Hospital	HG 3	n/a	-16.7%	**-80.4%**	330	275	54
Letterkenny University Hospital	HG 5	n/a	-11.4%	**-54.8%**	457	405	183
Mayo University Hospital	HG 5	n/a	-12.8%	**-44.6%**	321	280	155
Portiuncula University Hospital	HG 5	n/a	87.3%	**-33.9%**	118	221	146
Cork University Maternity Hospital	HG 4	n/a	2950.0%	**-29.2%**	12	366	259
Connolly Hospital Blanchardstown	HG 1	n/a	97.8%	**-18.7%**	225	445	362
St. Michael's Hospital, Dun Laoghaire	HG 3	n/a	182.1%	**-16.5%**	28	79	66
The Coombe Women & Infant University Hospital	HG 2	n/a	19.0%	**-15.3%**	263	313	265
St. John's Hospital, Limerick	HG 6	n/a	78.7%	**-13.1%**	47	84	73
National Maternity Hospital	HG 3	n/a	-57.0%	**-12.1%**	747	321	282
University Hospital Limerick	HG 6	n/a	0.3%	**-11.8%**	592	594	524
Sligo University Hospital	HG 5	n/a	-39.1%	**-3.5%**	470	286	276
St. James's Hospital	HG 2	n/a	-28.5%	**-2.7%**	991	709	690

Table 1: Hospitals showing drop in number of incidents reported from 2020 to 2021 for the period of 1st July to 23rdAugust*

***Note:** This table excludes Covid locations.

CHO Areas – A total of 3 CHO Areas (at Location Level 3) have shown a decrease in number of incidents reported from 1st July to 23rd August for 2021 compared to the same period in 2020. The largest drop is in CHO Area 6 – Voluntary, due to Sunbeam House Services reporting 181 incidents in 2021 compared to 382 incidents in 2020. CHO Area 7 – HSE shows a drop of 44.9%, mainly due to Cherry Orchard Hospital and Bellavilla Community showing largest drops in the number of incidents reported. Graph 4 shows the low numbers reported in May and June 2021 before the spike in reporting in July.

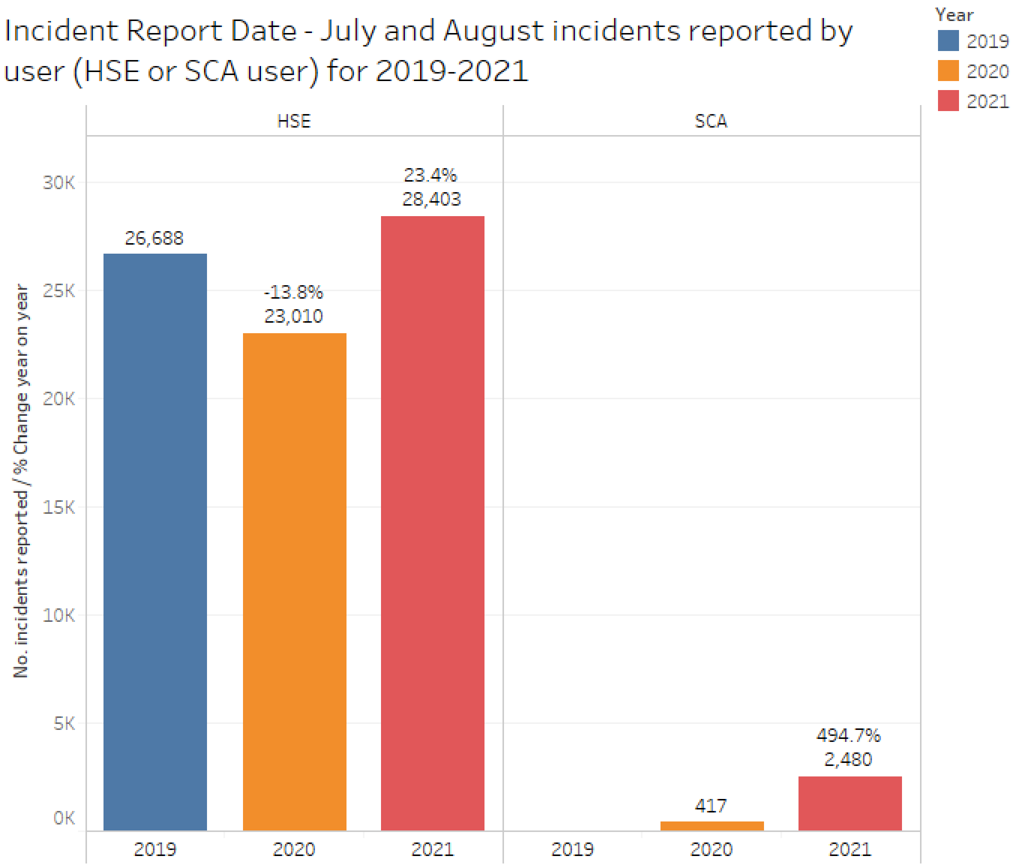
CHO AREA – Location Level 3	% Difference from previous year			Number of Incidents reported		
	2019	2020	2021	2019	2020	2021
CHO Area 6 - Voluntary - Wicklow/Dun Laoghaire/Dublin South East	n/a	-6.60%	**-49.60%**	412	385	194
CHO Area 7 - HSE - Kildare/West Wicklow/Dublin West/South City/South West	n/a	3.10%	**-34.90%**	641	661	430
CHO Area 4 - Voluntary - Cork/Kerry	n/a	-42.30%	**-6.50%**	612	353	330

Table 2: CHO Areas showing drop in number of incidents reported from 2020 to 2021 for the period of 1st July to 23rd August*

***Note:** This table excludes Covid locations.

Incidents eported for 1st July to 23rd August year on year for 2019-2021 by"who recorded the incident"

There is an increase in incidents recorded from 1st July to 23rd August for 2021 compared to the sameperiod in 2020 for both HSE and SCA users. HSE users reported 13.8% less in 2020 than 2019 but in 2021 reported the highest total of the 3 years. SCA users also entered incidents in 2020 and 2021 and shown a 494.7% increase in 2021. The SCA users entered 11.5% of the total incidents for 2021.

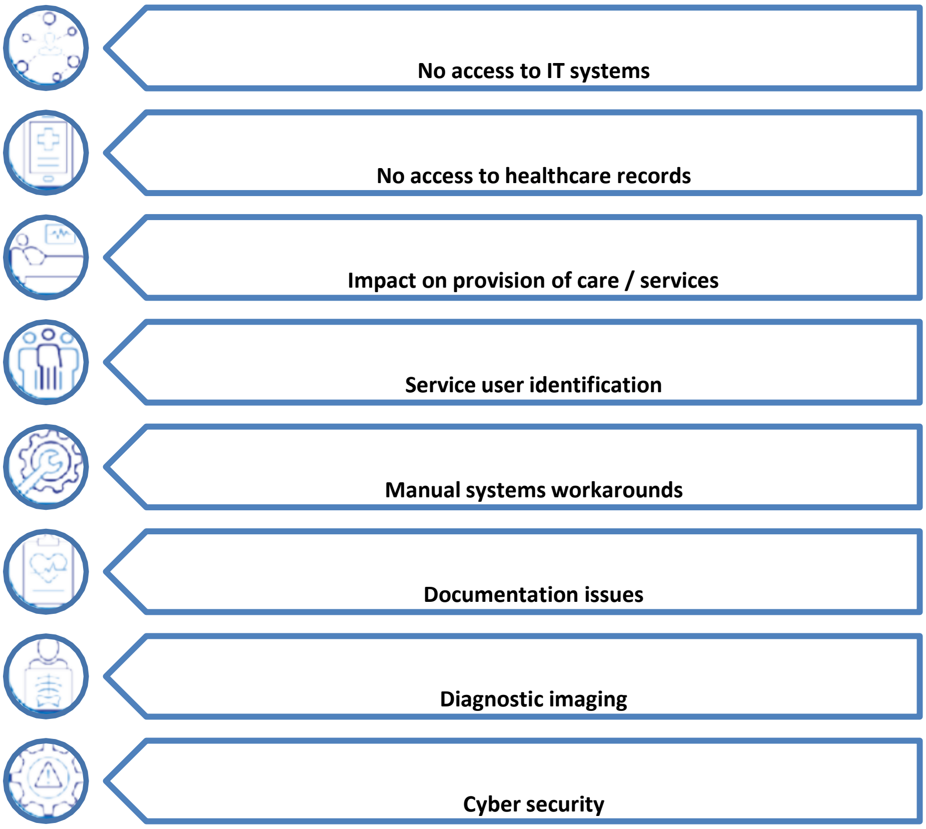


Graph 7: Incidents recorded by HSE or SCA user for 1st July to 23rd August for years 2019 - 2021

Qualitative analysis of cyber-attack related service user incidents

On receipt of NIRFS by the SCA, incidents were uploaded to NIMS by four business units within the SCA and a quality assurance (QA) process was undertaken by risk advisors as incidents were being uploaded. During the course of QA, a sample of service user incidents (those QA'd by the Clinical RiskUnit) were further analysed to identify incidents directly related to the cyber-attack itself. Some incidents were also identified by a keyword search. This yielded a sample of 244 incidents. A theme was applied to these service user incidents based upon the information that was available in the summary of the incident. The themes identified, in descending order of frequency, along with more detailed information on each theme, are presented below. Given the small number of incidents in this sample, the relative frequency of incidents should be treated with caution.

Themes identified



No access to IT systems

No access to healthcare records

Impact on provision of care / services

Service user identification

Manual systems workarounds

Documentation issues

Diagnostic imaging

Cyber security

Type of incidents by theme

No access to IT systems

Administration / Communication	Clinical care and patient information systems	Laboratory systems
• Unable to send communications to other health and social care services • Non-completion of COVID-19 pre-assessment questionnaire • Incident reporting system unavailable	• No access to electronic Healthcare Records (HCRs) • No access to patient information systems e.g. IPMS, NIMIS, Compuscope system • Unable to access or compare previous blood findings, radiological imagesand diagnostic test findings • No access to review service user infection control status	• Delay processing of all samples including COVID-19 swabs • No electronic lab findings,no mechanism to notify regarding infectious diseases • No labels available • No access to Blood Track, Healthlink, REES email system • Critical findings not communicated

Summary of an incident extracted from NIMS relevant to this theme:

‘Surgeon unable to view x-rays as a finding of the HSE Cyber-attack. Patient and instruments wereprepared for surgery. Discovered after screening that a different surgery was required’.

No access to healthcare records

- Physical or electronic healthcare record (HCR) not available / unable to locate HCR
- No access to previous medical / surgical history
- Incorrect medication prescribed and administered
- Potential delayed diagnosis / treatment

Summary of an incident extracted from NIMS relevant to this theme:

‘Unable to locate patient temp chart due to cyber-attack, lab findings returned from micro-e-coli UTI.Unsure if TX given or patient history’.

Impact on provision of care / services

- Delayed treatment / diagnosis e.g. pulmonary embolism, fracture
- Cancellation of appointments / procedures / services
- Service users attending clinic on wrong or unaware of cancellation of clinic
- Omission of service users names on theatre lists
- Delayed triage of service users referrals
- Birth notification delayed due to lack of fax / email services
- Procedure delayed e.g. no access to Endobag system
- Lack of access to teleconference facilities for medical consultation

Summary of an incident extracted from NIMS relevant to this theme:

'Surgery postponed due to clinical details not being available on patient due to cyber-attack. Explanation provided to patient'.

Service user identification

- Incorrect service user identifiers on documentation, request forms, laboratory findings, wristbands e.g. date of birth, name and spelling, medical record number, address errors
- Incorrect service user names on theatre lists
- Duplicate medical record numbers provided e.g. assigned to another service user
- No access to barcoded wristbands

Summary of an incident extracted from NIMS relevant to this theme:

'Incorrect date of birth and MRN on patient lab reports'.

Manual systems workarounds

- Manual labelling / recording / reporting - transcriptional errors
- Manual delivery of findings to wards e.g. misplaced findings leading to data protection issue
- Manual referrals
- Samples with incomplete information not processed, repeat samples required
- Delayed availability of findings
- Provision or review of findings for the wrong service user

Summary of an incident extracted from NIMS relevant to this theme:

'Unavailability of unisoft / track and trace due to HSE cyber-attack. Report written manually'

- Documentation in the wrong Healthcare Record (HCR)
- Incorrect service user identifiers
- Illegible handwriting
- Request forms missing important information e.g. not signed
- Medication kardex missing
- Misfiled records
- No addressograph labels available

Summary of an incident extracted from NIMS relevant to this theme:

'Various documentation issues during cyber-attack, missing and wrong PCN's, misfiled records, no stickers, incorrect DOB's etc. all issues resolved by staff eventually'.

- NIMIS not available
- Suboptimal image quality and without access to prior imaging
- Accumulation of studies requiring formal reporting
- Cancellation of services (urgent / scheduled)
- Delayed access to services
- Paper referral form not signed / not processed
- Incorrect procedure performed
- Unrecoverable loss of patient records / images, backup system corrupted

Summary of an incident extracted from NIMS relevant to this theme:

‘Large unreported volume, general x-ray 1247- risk delay diagnosis. CT: 96 unreported, US: 103 unreported. System slow since cyber-attack. Medical largely off line’.

Cybersecurity

- Unsolicited phone calls
- Request for SU credit card details
- Data breach

Summary of an incident extracted from NIMS relevant to this theme:

‘Reported by Consultant Urologist who received a phone call from a patient who advised that the person said was calling from hospital and advising patient to give credit card details to pay for a CT Scan in advance. GM phoned & assured the patient that they would never request payment in advance of treatment over the phone. Advised patient to report to Gardaí and hospital reported to Gardaí & to Hospital Group in light of recent Cyber-attack’.

Definitions:

National Incident Management System (NIMS): Incidents (which include claims) are reported using the “National Incident Management System”. This is hosted by the State Claims Agency (SCA) for the HSE, other Healthcare enterprises and Delegated State Authorities. An incidentcan be a harmful Incident (Adverse Event), no harm incident, near miss, dangerous occurrence (reportable circumstance) or complaint. An Incident can relate to a person, property, crash/collision,dangerous occurrence or complaint.

Date of Incident: The date the incident occurred, or the date of knowledge for chronic exposure(e.g. asbestos). For example, if someone slipped on Jan 1st 2001, the "Date of Incident" is 01/01/01.

Incident Report Date: the date the incident was entered on NIMS

Who was involved: Field detailing the type of person involved, e.g. Staff Member, Member ofthe Public, etc. This is the highest level of person category on NIMS, as displayed below.

Who Was Involved --> Category of Person --> Sub-Category of Person.

Appendix 6a: CHO4 AAR

CHO Cyber-attack AAR Summary Report Template on Patient Safety and Risk Management.

The template should be completed following a CHO AAR Meeting. You may attach any supplemental information you would like to be considered (risk assessments / registers *etc.*) as appendices. The core report should not exceed 5000 words (approx. 10 pages) excluding the appendices.

After Action Review Learning Report on Patient Safety & Risk Management in CHOs in response to the 2021 Cyber-attack

CHO Name or Number:	Cork Kerry Community Healthcare (CHO 4)
Date of meeting:	13th July 2021
Appendices:	Appendix 1 CKCH RAG Reporting Template @ 13th July 2021.

Background to AAR

Please provide a summary of the CHO initial response from day 1, and how this evolved. Focus on the questions below - relfecting for each on what you expected to happen, what worked well i.e. the expected outcome was achieved, and what didn't work well i.e. the intended outcome, for example control or reduction of a specific risk was not achieved by the agreed control. Then, focus on why response actions worked well or did not work, and what that means for future cyber-attacks or major systems outages and the CHO response.

Question 1 - Response, Risk Identification & Management.

What actions were taken from day one to identify and manage risk? What PPPG did you use, *e.g.* was the usual risk management or another process used, was it effective – *i.e.* did it finding in visibility and effective control. If not, why was this? How might this be improved for future cyber-attacks or major systems outages?

1. The initial response was managed within by the CHO Management Team governance structure when the cyber-attack was reported on 13th May 2021. Daily scheduled telephone calls to maintain oversight.
2. Local departmental /function emergency plans were activated but the cyber-attack was not managed in line with the National Emergency Management Process and this was a key deficit which resulted in a lack of co-ordination and duplication of efforts.
3. The CHO relied heavily on existing relationships with key (local) ICT personnel to assist the CHO response. This was an informal arrangement totally dependent upon personal relationships. The CHO required a senior named business partner in the OCIO on an ongoing basis who has a clear understanding and knowledge of all the ICT functionality available locally and would be the link person at a senior level for the CKCH Management Team the Chief Officer and for the new ICT GM role . This would provide better communication and coordination in the event of another cyber-attack and would be very effective on our local Crisis Management Team. This person should also be the link for the acute hospital services locally for intertwined systems etc.
4. The Chief Financial Officer set up a WhatsApp group on 17th May to allow for updates on Cyber-attack to be shared with senior finance colleagues across the CHO, HBS, Hospital

Groups, PCRS, Tusla etc. This was followed up with teleconferences three times a week at which OCIO Representative and SAP CoE Representative attended to give updates. A Log of finance issues was set up and updates on systems were given during the calls. Various subgroups were set up across finance functions around setting up processes to deal with emergency AP Payments, Payroll, system issues, etc. Many issues have been resolved or alternatives put in place, the frequency of meetings have been reduced to once weekly with key links in place in case of issues arising in between

5. The HSE's Chief Clinical Officer provided guidance to all clinicians on patient safety and priority focus while our services respond to this attack on 25th June 2021
6. Additional teleconferencing capacity was sourced locally (through the CMT) to enable communication across the CHO due to the complete lack of access to internet and email.
7. All services risk assessed the impact of the cyber-attack and identified controls to mitigate the risks in so far as possible in line with the HSE Risk Management Policy. An operational and clinical risk log was established to provide the CHO Management Team with a high level overview of the key risk areas within each care group.
8. RAG template returns to the National Director of Community Operations.
9. A CKCH cyber ICT Lead was nominated by the Chief Officer as per the direction of the National Director, Community Operations
10. Information was shared by the Chief Officer from National MT calls on a regular basis.
11. Crisis Management Team was a forum to glean information internally to CKCH and SSWHG
12. National OCIO/CHO Meetings began 5 weeks after cyber-attack on 14 June 2021.

Question 2 - Clinical and Operational Risks.

What clinical risks, or groups of similar risks, did you identify and what specific system outage caused each? What were the controls you put in place for each, how quickly could you put these controls in place and were they effective? If not, how could this be improved for future cyber-attacks or major systems outages.

1. **Covid Testing & Community Vaccination Programme**
   - Swiftque outage impacted upon our ability to log and process covid swab requests. Lack of access to the scheduling facility meant that all test centres had to operate a walk in service which led to a lot of duplication and increased need for admin resource.
   - Contact tracing facility was also inaccessible and the reliance to communicate to close contacts fell to the individual being tested.
   - An increase in covid testing requirements was noted across Cork & Kerry and pop up testing centres were put in place to manage the increase in testing requirements.
   - The lack of access to the PPE ordering facility was managed by issuing a repeat of the previous order to all facilities. Emergency orders were communicated via telephone.
   - The PPE System is still down and not due back until 29/7 – of concern as surge has commenced
   - Challenges in delivering upon the community vaccination programme due to our ability to order vaccines and a noted increase in DNA rates potentially attributed to individuals assuming clinics not progressing due to cyber-attack.
   - Unavailability of regional laboratories lead to all Covid swabs going to ENFER and external facilities for a number of weeks

2. **Covid Response Team (CRT)**

- Challenges in accessing clinical and operational information stored on shared drives and a lack of email facility created difficulties in communicating with private nursing homes. Twice weekly telephone contact with 58 private nursing homes facilitated by the CRT members to maintain contact and support.
- Contingency planning visits to private nursing homes continuing with paper based reports being produced.
- Unable to access Nursing Home Pathway data base so referrals had to be uploaded retrospectively.
- CRT National Covid Portal inactivated. National CRT Lead contacted if there were issues to escalate around outbreaks.
- Healthlink outage impacted GP's of Private Nursing Homes being able to request Covid tests for residents. All swab requests had to go through the CRT and then directly to testing team to create swift Queue numbers.

3. **Laboratory findings (LIMS, PAL and PHML)**

- Limited or no access to previous laboratory findings presented increased risks in patient care decisions that needed to be made in the absence of laboratory findings.
- Emergency laboratory findings facilitated but routine blood tests delayed.
- Prescribing Clozapine machines are linked to IT and these blood test findings are urgent with high risk.
- Renewing prescriptions was an issue with not having access to laboratory test findings.
- Abnormal findings being communicated by phone, fax and post.

4. **Dental Service ICT System (Soel and Fire Eye)**

- Lack of ICT systems has impacted on the service's ability to attach photographs and x-rays.
- Retrospective uploading of manual records to be prioritised.
- Lack of email and access to waiting list information is critical.

5. **Time sensitive clinical referrals to Public Health Nursing Service**

- Risks of delayed referral for urgent time sensitive clinical child health procedures i.e. new born blood spot test.
- Significant challenges in managing referrals, accessing patient information which is leading to delays in delivering public health nursing services.

6. **Audiology (PMS – Audit based/linked to NOAH)**

- Audiology services curtailed due to some diagnostic instruments requiring network access to function. No workaround solution available in the interim.

7. **Podiatry (Tyndale System)**

- Lack of access to Tyndale system (record management / clinical record) - podiatry services curtailed due lack of access

8. **GPs / OOH (Health link)**

- Lack of access to Health link/diagnostics/labs/faxes etc. significant curtailment of services. Interim solutions put in with private providers re diagnostics / urgent labs prioritised reverted to phone contact in the majority of work.
- Online MHS referrals from GPs were not transmitted on healthlink and MHS were not aware that referrals had been made. This posed risks to patients who may have required assessment and treatment.

9. Palliative Care / CIT

- Lack of access to diagnostics / patient record systems / lack of radiotherapy services/ labs / pharmacy – reverted to manual recordings: lab work ups/patient records etc.

10. Pharmacy

- Integrated system disrupted, lack of access to faxes – reliant on telephone contacts hence associated increased risks.

11. Orthodontic Service (Orthotrac & T Doc digital tracking system)

- Lack of access to the Orthotrac system impacted on ability to access photography and x ray diagnostic test facilities, impact on clinic activity
- T Doc digital tracking system has impacted services ability to trace instruments

12. Access to iPIMS & Managing Clinics

- Lack of visibility of patients on waiting lists.
- Revert to manual records in absence of access to iPIMS which means a considerable volume of hard copy records need to be retrospectively entered into the Patient Information Management System once it is restored.
- Challenges in delivering clinics across all services due to lack of access to ICT system for clinic lists, patient contact details, pulling patient files, issuing appointment letters and managing DNAs. Limited access to patient information to inform prioritisation for appointments.
- Telephone contact is being made with service users where telephone numbers are accessible. Media call out made to patients to make contact with the service to confirm their attendance at appointments.
- A process is being put in place to ensure that DNAs are checked.
- Paper based records are being kept for upload when patient management systems are accessible.

13. Infection Prevention & Control

- IPC team contactable by phone line for services to seek guidance advice and support.
- IPC team provided support and guidance to frontline staff in the absence of staff being able to access the HPSC website during the cyber-attack.
- IPC Site visits continue with reports being prepared manually.

14. Safeguarding Referrals (Lack of access to email, case management system and issues with encrypted emails being quarantined)

- Access to dedicated phone number remains in place while central email is accessible. Safeguarding team have notified key stakeholders in writing re how to access team (phone and registered post)
- Additional staff allocated to cover phone lines due to higher volume of calls.
- Notice re no email available due to cyber-attack placed on social media.
- Unable to access client information held on case management system. This has impacted on teams ability to schedule follow up appointments, case reviews etc.
- Team have reverted to using paper based case management system. A process for retrospectively uploading paper based files on the shared folder is planned.

15. Communications

- The Communications team had no access to email; mailing lists or other means of quickly issuing information to the media to alert the public about the impact on services. Initial updates to the public (via media) were issued verbally or by text message. An alternative email address was quickly put in place for outward communication, but this still had limitations. Emergency planning work was useful as printed versions of contact files were available. These will also be available to the off-line communications Gmail account in the future (i.e. in the event of another outage).
- The communications team couldn't access the usual channels to issue updates to staff (i.e. broadcast email). Other platforms including the CKCH social media accounts were used to good effect. There needs to be recognition of the importance of access to social media platforms for all staff especially in an emergency situation. Consider access to another platform i.e. staff app.
- Staff relied on personal devices and personal Wi-Fi in order to create and issue updates.

16. Printers

- All HSE printers were inaccessible as they were linked to devices and networked to facilitate multi use access. Printers were removed from networks and assessed to enable staff to access the copying function on an interim basis.
- Printer hubs were established across a number of sites with "clean" devices to enable staff to copy patient files, forms, letters etc.

17. Telecommunications

- This fundamental enabler to ensure an effective response was jeopardised, all teleconference systems were affected. Support was obtained from the local authorities; there is a necessity for resilient communications to absorb or mitigate the effects of a disruptive challenge.
- Franking machines are linked to online accounts for postage top ups. The increase in postage during the cyber-attack was hampered with difficulties in securing financial top ups for franking machines without access to the internet or online payments.

18. Smart phone order process postponed

- Inability to order new or replacement smart phones has impacted the service to communicate with new appointees. Staff are un-contactable particularly in the circumstances where staff do not have access to a landline due to insufficient office accommodation.

19. Telemedicine

- Remote telemedicine forums were inaccessible which led to appointments being cancelled or postponed. Work commenced nationally on enabling key telemedicine tools to be made available for use on the personal devices used by staff as an interim measure.

20. Mental Health Tribunals

- Information pertaining to patients who require an urgent involuntary admission was delayed due to lack of ICT system. Tribunal services were maintained with patient files being copied to the tribunals and faxed or sent via registered post.

21. Notifications to Regulatory bodies (HSA, HIQA & MHC)

- Notification made to the Health & Safety Authority (HSA) via telephone while the online portal for reporting incidents was inaccessible.
- Statutory notifications made via telephone and registered post in line with HIQA/MHC instructions in absence of online portals.
- Communication pathway / protocol was established between HSE and MHC.

22. National Incident Management System (NIMS & CMS)

- Incident reporting on NIMS portal inaccessible for incidents and complaints which has impacted on compliance with incident and complaint reporting timelines.
- Manual NIRFs made available to all services and SAOs notified of incidents via telephone.
- Plans in place to upload any backlogs of incidents when NIMS portal is accessible.

23. Delays in assessments of need (under the Disability Act 2005)

- Delays arising from the inability to access files and schedule appointments which is in non-compliance with the Act. Progressing cases based on hard copy information and working closely with private service providers on AON requirements.

24. Community Schemes ICT Systems

- Manual work around process put in place for emergency scheme payments and online application forums reverted to manual forms for emergency requests.
- Backlog of payments e.g. COSS, EHIC and Hardship scheme to be uploaded once ICT system becomes available.

25. Registration ICT System – CRS

- Registration of births, deaths and marriages were impacted. Manual process put in place for emergency requests and any delays in social welfare payments and overpayment for deceased persons will be prioritised when ICT system access resumes.

26. School leavers placements

- Inability to access the school leaver’s database will lead to delays which in turn may delay new services being identified.
- National system is also interlinked to the allocation of indicative funding function.

- Progressing work based on keeping manual systems.
- Liaising with National Office regarding indicative funding for new profiled school leavers.
- Engaging with agencies regarding negotiations to progress planning of new services.

27. Health and Wellbeing

- The majority of client facing programmes had been moved on line due to Covid and this contingency plan was significantly impacted by the cyber-attack. The lack of availability of client files, Outlook diary information, and video conferencing facilities impacted the delivery of services such as QUIT and Self-Management Support Training. Smoking cessation support for clients with diagnoses of cancer was prioritised insofar as manual records allowed.
- There was a major reliance on staff using personal WiFi and internet facilities to continue a reduced level of service.

28. Referrals to Home Support

- Significant challenges in receiving referrals from the acute hospitals and community services. This was further impacted as the request for service from the Private Providers could not be issued collectively by email as per tender and each had to be contacted individually. This resulted in delays to delivery of service.

29. A&TC/ Ambulatory Outreach/ ICPOP Kerry:

- Lack of access to patient records, diagnostics, labs, iPIMS and TPro significantly impacted service delivery.

30. Nursing Home Support System(NHSS)

- Lack of access led no visibility of the Nursing Home Support Scheme.

31. HR

- On-going delays in progressing Winter Plan and National Service Programme Recruitment campaigns owing to non-availability of full ICT.
- Delays to business case processes associated with backfilling vacant positions.
- Head of HR continues to engage with Service Management, Central Payroll, Central Pensions, Personnel Administration and relevant Trade Unions where required.
- Office of Head of HR - Workforce Resource Unit liaising with NRS and Managed Service Programme (MSP) to progress recruitment campaigns where possible. Notices issues via Social Media to advise potential candidates Manual payroll sheets currently in operation.
- Head of HR continues to engage with Service Management, Central Payroll, Central Pensions, Personnel Office of Head of HR - Workforce Resource Unit liaising with NRS and Managed Service Programme (MSP) to progress recruitment campaigns where possible. Notices issues via Social Media to advise potential candidates of extended timelines for submission of applications.

32. Payroll

- The risk to potential delays in payments being made to staff in line with terms and conditions of employment is being reducing in line with the incremental improvements to ICT access and to the high level of support provided to Line Managers, Payroll Returning

Officers by Central Payroll in HSE South.

- On-going potential for over/under payments being made due to inconsistency of availability of ICT systems.
- Processing of travel expenses on hold pending access to ICT systems.
- Access to Payroll History, Personnel Records ('Therefore'), Census data, attendance/absenteeism ICT systems etc. incrementally improving however, as not all services have access to relevant ICT systems, current HR reports not available to central HR. Delays to full return are impacting service delivery to support the processing of HR schemes, entitlements e.g. Parental Leave, Maternity Leave, Long Term illness Schemes, Pensions, etc. Payroll returns currently being processed manually.
- Pensions & PA Sections continue to accept paper based applications via relevant HR Forms where email access not available.
- Head of HR continues to engage with Service Management, Central Payroll and Central Pensions to address any payroll issues.

33. Home Support Payroll (Rivendale Database)

- Lack of access to the Rivendale Database impacted on the payment of HCSAs for pay period 24 and 28. Pay period 24 will have to be reconciled which creates a significant increase in workload in advance of progressing the payment of future pay periods.

34. Accounts Payable

- Usual payment systems compromised affecting payments to clients and contractors. Workaround put in place with Finance function within the CHO to address urgent, essential, and time bound payments. Work is ongoing with IT around transferring payment data from Creditors to Finance Systems by External IT Provider

35. Payments to Service Providers (under Service Arrangements)

- Lack of access to ICT delayed scheduled payments to HSE funded agencies. Workaround solution established by Finance enabled essential payments to be processed on an interim basis.

36. Patient Private Property System (Citrix)

- This system holds details on all transactions for individual clients financial transactions, lodging of pensions, charges, bank account balances, etc. List of Computers with bank account details have been submitted to Treasury
- Local Areas hold manual records while no access to systems and update system when access restored. This will enable residents to have access to their money.
- Workaround using intranet access has been established to access system on an interim basis.

37. Finance (month end financial reporting requirements)

- Delays in completing financial returns with catch up in data gathering when all systems become available. Workaround being done to complete month end with estimates, manual data gathering, etc. On-going engagements between all Finance Divisions, IT and CFO to work on resolutions.
- Data gathering of IT Systems where large quantities of banking details are held and will be

submitted back to HSE Treasury Department.

Question 3 - Support for CHO Response.

What functions, teams or providers did you have critical dependencies on to manage risk? Did you receive the support required and was this effective? How could this be improved for future cyber-attacks and major systems outages.

1. Local CKCH Area Management Emergency Management Plans needs to be reviewed to ensure continuation of service provision, this event highlighted weakness in contingency plans
2. The CHO required a senior named business partner in the OCIO on an ongoing basis who has a clear understanding and knowledge of all the ICT functionality available locally and would be the link person at a senior level for the CKCH Management Team the Chief Officer and for the new ICT GM role . This would provide better communication and coordination in the event of another cyber-attack and would be very effective on our local Crisis Management Team. This person should also be the link for the acute hospital services locally for intertwined systems etc.
3. Meetings commenced between OoCIO and CHO five weeks into the Cyber-attack.
4. Text messaging service to all users was in theory, a good way to get information to staff, but unfortunately mixed messages from this source lead to confusion across services. The one size fits all messaging approach didn't meet our requirements. The messaging service didn't differentiate between ICT systems in use across the service which meant that some instructions were not relevant or applicable as solutions.
5. Lack of independent WIFI access to enable communications proved unhelpful, and there was an over reliance on staff using personal WiFi , hotspots and internet facilities to maintain basic communications and enable service delivery.
6. High reliance upon PFH and the army to deliver onsite device cyber checks on site. This worked well where staff could be accommodated on site but not when accommodation didn't allow for all staff to be on site at the one time (Social distancing requirements due to Covid working environment). No visibility of when the onsite scanning was being undertaken.
7. The ICT Helpdesk was available to staff as support, but the staff working in the centralised service were not always aware of the systems in use in our area. In some instances, the central ICT Helpdesk was not aware of local instructions i.e. users were notified locally to connect their devices to commence the decryption process. Staff who encountered issues contacted the help desk to be told to disconnect their devices immediately which was the opposite to instructions issued locally.
8. ICT in the Cork Kerry region is not as advanced as in other CHOs. There are a number of legacy ICT system in place which have no back up facility and are largely unsupported systems. Local knowledge and local solutions to local issues came into play in order to ensure both systems and data were screened and protected to support essential services.

Key Learning Points Identified

For each of the questions above please flag any lessons you learned about what worked well and agree CHO actions and/or make any recommendtaions for how this learning could inform futrure response with a view to preventing harm to servivce users, residents and patients.

For each of the questions above please flag any lessons you learned about what did not work well and agree CHO actions and/or make any recommentaions for how this learning could inform future reponse and prevent harm to service users, residents and patients.

1. Local CKCH Area Management Emergency Management Plans needs to be reviewed to ensure continuation of service provision, this event highlighted weakness in contingency plans.
2. The CHO required a senior named business partner in the OCIO on an ongoing basis who has a clear understanding and knowledge of all the ICT functionality available locally and would be the link person at a senior level for the CKCH Management Team the Chief Officer and for the new ICT GM role . This would provide better communication and coordination in the event of another cyber-attack and would be very effective on our local Crisis Management Team. This person should also be the link for the acute hospital services locally for intertwined systems etc.
3. Cyber-attack should have been managed in line with the National Emergency Management process.
4. The reliance on one mobile phone provider for all phones and for mobile internet could lead to a situation where there is no back-up systems in the event of a widespread outage on one network.
5. Lack of knowledge on what systems are in place within the CHOs proved problematic. ICT staff depended on local knowledge to identify systems, locations on servers etc.
6. CKCH is currently not on SAP HR or HealthIrl which meant that we weren't affected when these systems were impacted. That being said, it is our understanding that services who are on these systems had to come to one central hub in Dublin to access the system. If and when our CHO moves to SAP HR and HealthIrl, we would expect that regional hubs would be established should a future cyber-attack or system failure arise in the future.
7. The Crisis Management Team was not fully enabled to establish the "current recognised situation" which is the starting point for dealing with any crisis. It was totally reliant on existing teleconference facilities and local relationships with IT personnel for information. Fax machines were resurrected to address some of the gaps in communication capacity. This was reliant on other part of the services having fax machines. Tetra Radios are available in the event of the total failure of the telephone system – these link to NAS and Acute ED's. The default position is to physically come together and we are short of facilities to convene large groups for emergency purposes. Resilience and redundancy is required in future in regard to both ICT and Telecoms for this area if we are to have secure communication routes within the health service in Cork and Kerry.
8. IT literacy – assumptions were made that staff had a certain level of IT literacy to be able to follow instructions re decryption process and other work arounds to enable continutiy of services. Some staff were able to engage with this but others were not.

Agree CHO Actions and Make Recommendations for National Community Operations Here

The actions and / or recommenations should be linked to the learning points identified above.

1. The CHO required a senior named business partner in the OCIO on an ongoing basis who has a clear understanding and knowledge of all the ICT functionality available locally and would be the link person at a senior level for the CKCH Management Team the Chief Officer and for the new ICT GM role . This would provide better communication and coordination in the event of another cyber-attack and would be very effective on our local Crisis Management Team. This person should also be the link for the acute hospital services locally for intertwined systems etc.
2. The Cyber-attack should have been managed in line with the National Emergency Management process.
3. Emergency Planning – secure location, IT and Telecoms for the future incidents & we need to be able to access alternative WIFI without relying on staff personal devices.
4. It is essential that the OoCIO carry out an audit or mapping exercise to identify the list of ICT systems, servers etc. in each CHO so that the OoCIO is aware of and have knowledge of systems on the ground.
5. Alternative methods of communicating with staff i.e. back up WiFi, access to multiple mobile networks.
6. Consideration needs to be given to cloud based back up solutions as well as back up servers.
7. There is a requirement to have a schedule of robust tesing of regional/local emergency plans in line with the Emergency Management Framework. This would ensure that similar crisises could be managed inline with pre determined plans rather and fire fighting during a crisis.

Appendix 6b: UHLG AAR

Cyber-attack

11/08/2021

What did we expected would happen?

- That we would revert to paper processes.
- Systems to view images wouldn’t be available
- That we would develop a Risk Register for the cyber-attack for the Group.
- That we would have patient safety incidents.
- That we would revert to manual pro cesses for incidents and complaints.
- To put the patient first and continue to focus on patient safety and their experience protected throughout their Hospital journey.
- Expected full oversight of clinical systems and back up of systems/
- Expected more knowledge/awareness of virus’ – IT software knowledge e.g. use of USB memory sticks.
- To have a back up or systems to protect our clinical systems – that systems could be deactivated and reactivated in protected mode a lot quicker.
- Proactive, energetic approach to patient safety.
- Assumed clinical systems would be robust enough to withstand an attack.
- Expected anti-virus software would have worked and protected the clinical systems.
- That we would have had stand-alone clinical systems that could have been isolated and continued to use with some cut off.
- Impact and solution challenges were not anticipated.
- Challenge across ICT and CHO areas of responsibility/governance.
- Swifter response to resolve the issues caused by the attack.
- That Covid 198 prepared us for the emergency.
- That contingency plans would kick in.

What Actually Happened?

- The scale of the impact was only fully understood as patient services struggled in the early days to cope with the attack.
- Further impact on scheduled and unscheduled care following impact of Covid 19.
- Clinicians were making decisions with limited information and access to patient information.
- Clinicians walked to various departments to view patient information available due to local access only.
- A Group Risk Register was developed for the cyber-attack.
- Manual processes were introduced for raising incidents and complaints.
- HCI and States Claims Agency assisted with uploading of information.
- HCMT was stood up across the Group.
- Patient safety was at the centre of everything that we did.
- Great leadership and cooperation across all grades of staff.
- Flexibility in work patterns – changes in rosters, weekend working, longer days.
- Very few patient safety incidents were reported.
- Paper systems were introduced and work rounds developed and tweaked as necessary.
- Finance – no restrictions – what was required was approved, great co-operation.
- Work rounds – introduced and tweaked as necessary.
- ICT – very supportive with limited resources on the ground.
- Lab has local system experts on site.

- Commend ICT who prioritised areas and looked at key components and systems to attend to first.
- No visibility of what patients were due to attend across all services i.e. opd, cancer services, elective surgery.
- Concerns and difficulties as the pharmacy systems e.g. Cliniscript were compromised, we were relying on previous scripts for cancer treatment patients in the initial phase. Need complartimentilasation of clinical systems.
- The number of ICT systems and they were all impacted and in trouble, no way to isolate systems.
- Servers – magnitude of data stored on shared drives that were no longer available.
- Challenges around ICT governance – UHL/Model 2 sites and the allocation of resources.
- We had lost sight of the manual processes to be introduced and some new/inexperienced staff had no experience of manual systems.
- Model 2 sites not resourced.
- Impact of cancellations, charts not being available, no ability to view X Rays – huge clinical risk – concern about when the full impact of this will become apparent.
- Worse impact than Covid 19.
- Felt the impact on Patient Safety was played down at a National level.
- Number of shared drives lost.
- ICT resources were very stretched.
- Disaster recovery plan – is there one?
- Communication challenges – huge dependency on emails as main form of communication, email being used as a live repository for storing vast amounts of information some going back years.
- DO not have a robust medical records process in the event of a systems failure.
- Medical Records – IPIMs dependency – lack of IPIMs support on site, external companies used for chart lists if available, work rounds were very labour intensive and time consuming and had to be designed as none existed– managing people's expectations was very difficult, up to 15,000 medical records stored throughout the Hospital.
- PID numbers for patient presenting could not be generated, V numbers were developed.
- Continued difficulties merging V numbers, concerns about the reliability of the track and trace system, ongoing process to tidy up after the attack and continue to manage staffs expectations.
- Backloading – no involvement in designing the process but have to implement it and make it work.
- Impact on scheduled and unscheduled care including OPD and virtual clinics – beginning to feel the effects and will for some time to come.
- Effect on general practise – which impacted on ED attendances and continues to impact.
- Could not generate electronic discharge letters for GP's.
- Unable to process routine bloods for GP's, emergency bloods prioritised.
- GP's had to revert to manual processes as clinical systems not available to them.
- Delays in reporting as clinical systems not available.
- Staff redeployed to various departments depending on the clinical need i.e. lab, radiology, ED, medical records and the wards.
- Staff were also redeployed to process payroll runs.
- Patient flow issues, delays in reporting, delays accessing images.
- Reconciliation pathway and plans to address the backlog.
- ED ICNET in particular as lack of access caused patient safety concerns.
- ED patient records could not be uploaded onto our document control shared file, Therefore. A room had to be set up to manually manage the patient records.

- Time consuming manual work rounds for consumables/services.
- Due to Lab accreditation - they had a manual back up system that kicked in immediately which generated paper reports that were delivered to the various departments.

Why there was a difference?

- Lack of preparation for such an attack and lack of a back up plan.
- No cyber-attack training or trial run for any staff.
- Patients and relatives were further isolated as many of the wards phones were connected to the IT system and it took a number of days to restore limited phones for essential clinical use.
- Work Rounds in place for some clinical systems but not all.
- Staff throughout the Group did everything possible to keep patients as safe as possible.
- Staff ensured verbal communication with patients as much as possible.
- Some Work Rounds that we in place were compromised as all clinical systems were down.
- Never imagined it could happen and the impact be so immense.
- Scale of attack unprecedented – used to some systems going down but not all clinical systems.
- Length and impact of the attack unprecedented.
- Piecemeal process to dealing with the attack, no joined up thinking/back up plan.
- Governance was an issue – reliance on CIO, segmented approach.
- Lack of compartmentalisation of clinical systems/hospitals (St. Johns and St. James were able to compartmentalise their clinical systems which lessened the impact.
- National approach – easier decision to link all sites/group at the expense of cyber safety – best practise would suggest compartmentalisation is a better and safer option).
- EHR per discipline – there are numerous different parts of the EHR across the Hospital Group e.g. renal, elderly medicine, Medonc, ED, Maxiums, Cardiology.
- Lack of ICT cover available for the community – reliance on UHL resources.
- Fingerprint – cannot be updated manually, log had to be maintained.
- Out of date systems – Microsoft 10 needed and would have sped up recovery if available throughout, level of IT support for a National Radiology system.
- Communications – severely impacted, some HSE phones could not facilitate Whatsapp so staff had to use personal mobiles, staff app vital, wifi an issue.
- Staff had to use personal emails and laptops.
- Lack of preparation locally and nationally.
- Nationally response not what was expected – being told months not days for recovery.
- Very little information about personnel information being released.

What can be learned?

- Major emergency plan needs to be developed for a cyber-attack and any other conceivable attacks the organisation could face.
- Emergency plan/crisis plan to be introduced and tested regularly.
- We are very good at crisis management and adapt well when faced with a crisis.
- Good leadership was shown throughout and everyone worked very well together to deliver what was expected from us and our areas of responsibility.
- Need to have a comprehensive plan and list of process/work rounds to be implemented and standardised across the Group and Nationally.(National Work Around document)
- Each department needs to develop their own manual work round processes in the event of a future cyber-attack that are regularly reviewed and updated.
- Training piece needed on manual process and work rounds for all staff.
- Requests for local and national data needs to be streamlined – with no access to secure PC's and emails– requests should be limited to essential information required only – lot of pressure to produce information requested from multiple sources.
- Duplication of information requests.

- Issues with electronic rosters – no visibility when systems went down.
- Rolling upgrade of ICT infrastructure needs to be planned nationally and locally.
- Relevant apps need to be available on hospital mobiles.
- Concerns about using gmail and personal laptops to transfer confidential information.
- Reliance of emails a concern – volume of data/information stored in emails – need to consider alternative options.
- Emergency IT response with the ability to isolate clinical systems so certain vital functions can remain operational e.g. images, labs, charts, contact patients.
- Governance for the ICT across the Group to be addressed.
- Comms were informing the public as necessary – have they any feedback?
- OCIO – Cloud First Policy – need to progress the Microsoft cloud offering as a strategic direction both locally and nationally to reduce attack surface area.
- External companies ICT support – need a robust plan as we were vulnerable, security service is provided by the OCIO and firewall is collapsed into a single server.
- Compile a list of the specialist clinical systems in the hospital and who is the expert on each system – list of who has responsibility for each and this can be reviewed regularly.
- ICT Disaster Recovery Procedure – which is tested every 4/6 mths, dry runs and procedure reviewed every quarter.
- System for storing policies and procedures accessible when PC's are not.
- 1* access point for NHN connection is not sufficient.
- Lack of awareness of a cyber-attack needs to be addressed - education required– seriousness around the use of personnel laptops, gmail accounts, usb's.
- Complete review of waiting lists needs to be completed – OPD, elective, pre and post cyber-attack from a patient safety perspective.
- Major Emergency plan needs to include medical records.
- ISO manual process needs to be stood up.
- Variance between areas that are accredited and had manual processes and those that are not.

Appendix 6c: CHI AAR

AAR Summary Report Template

After Action Review Learning Report

Patient Safety following Cyber-attack 14th May 2021

Children's Health Ireland

Date of meeting: 19th July 2021

Background to AAR

CHI was severely Impacted by a Cyber-attack on 14th May 2021.

This AAR was estblished to identify learning points from an organisational perspective relating to patient safety following the Cyber-attack.

Key points discussed

- CHI was severely Impacted by the Cyber-attack
- The severity of the impact and recovery varied from site to site.
- CHI was impacted more severely than other HSE organisations.
- A major emergency type response was required - even though the event could not be described as clearly as a major emergency.
- Communication was challenged - staff at all levels expected communication but route of communication (ICT) had been wiped.
- Communication needed to happen from corporate level as well as locally/site based.
- Cross-site collaboration was good.
- Innovation and resilience happened quickly.
- Contingency/back-up plans were vital, led to success of recovery.
- Different groups of staff were communicated with in different ways - felt different in different sites.
- External communication (media, HSE) varied and did not seem to acknowledge severity of impact of attack in CHI
- This cyber-attack hurt staff, already impacted by 16 months of pandemic.
- This attack was emotive, it was an attack.
- Consideration needs to be given to why it happened so severely in CHI - vulnerability of organisation for the future.
- National systems recovered more urgently - learning for future systems within organisation
- Individuals responses had impact on recovery in positive way.

Additional discussion notes

What did we expect to happen?

- The organisation would move straight into disaster mode
- We thought CHI ICT would be able to sort it out for us
- That more of the consequences would have been anticipated
- That people would be resilient and adaptive
- That patient safety would be prioritised
- That there would be a lot of media coverage
- That local plans would be made for local activity
- That there would be a central place for communication and updates
- We thought that May 14th would be the day that the Children's Nursing Strategy was launched
- We expected that the impact would be the same on all sites
- We expected that it would be really obvious who was managing which parts of the Major Incident between CHI and HSE
- We expected that the incident would be over fairly quickly

What actually happened?

- It wasn't a clear cut incident as we didn't know the duration
- The Major Emergency Plan didn't really fit what we needed to do
- Patient Safety was prioritised
- The impact lasted much longer than we expected
- There were a lot of assumptions around the type of contingencies that would be available
- There was not as much media coverage as we expected, especially after the first few days
- Communication was very difficult, with limited central functions
- Every system was impacted and the loss of function In labs and radiology was instant and severe
- People were very innovative with workarounds Including buying IT equipment themselves to deliver the contingency services, and sharing the contingency plans across the country
- Everyone worked together
- Media coverage fell away pretty quickly, and didn't seem to reflect the high Impact In CHI
- There was limited external support response visible
- A lot of people didn't know how to contribute
- Losing every system was not our expectation of what was likely to go wrong In ICT. Previous experience was of losing one system at a time
- Staff were hurt by the intentional nature of the Incident
- Staff were frustrated and isolated by the nature and duration of the incident,

Why was there a difference?

- We had no experience of an incident like this and no real expectation that the global ICT shutdown was possible
- We didn't have an appropriate Business Continuity Plan In place
- CHIs older ICT Infrastructure seemed to be particularly vulnerable
- The incident came on the back of a service already strectched by COVID, and where bringing staff back In ot work on centrally connected ICT was not an Issue because of the need for social distancing.

Lessons Learned:

- That we need to invest in ICT and cyber security, especially until the more resilient EHR is in place
- We need to make sure that staff confidence in ICT resilience is maintained and even increased, so we don't see an increase in manual workarounds persisting.
- EHR needs to be strongly cyber-protected.
- There needs to be strong business continuity/contingency plans/culture in the organisation.
- There needs to be a plan for a second copy of the patient's HCR - that might mean patients having a copy of their own HCR.
- CHI need to return ICT services to 150% of standard prior to 14th May.
- There needs to be a plan to respond to breach of data.
- CHI needs to consider national ICT systems within the organisation.
- We need better local Major Incident Plans and a single CHI Major Incident plan

Actions Identified:

- CHI Cyber security capacity and capability to be increased by development of a Security Operations Centre (Chief Information Officer)
- Cyber-attack lessons will be incorporated into the ongoing procurement for the new EHR
- CHI reviewing all site Business Continuity and Major Emergency plans (Chief Operating Officer)
- CHI developing an integrated Organisational Major Emergency Plan to bring all the site plans together and design the full organisational response (Chief Operating Officer)
- CHI to ensure that ICT development plans are updated to include recovery needed from Cyber-attack (Chief Information Officer)
- CHI to complete Recovery and Restore phases of the Cyber-attack response and Data Breach management as planned (Chief Operating Officer)
- CHI Executive to develop communications plan to restore and develop ICT trust across workforce (Head of Corporate Affairs)

Kerry Russell

Director of Quality, Safety and Risk Management

Children’s Health Ireland

Engage with us on twitter @NationalQPS or by email at nqps@hse.ie