Freedom of Information Schedule of Records - Summary of Decision Making

FOI Request	MMUH Ref: 7095

Rec. No.	No. of pages	Date of Record	Brief description of record	Decision
1.	10	14 August 2024	ICT After Action Report 14 August 2024 v3_Redacted	Part Granted • Section 29 • Section 30 • Section 33
2.	7	14 August 2024	Root Cause Analysis Report for the Mater Misericordiae University Hospital (Mater)	Part Granted • Section 33 • Section 36

Mater Misericordiae University Hospital
Sisters of Mercy
Eccles Street, Dublin D07 R2WY, Ireland

Ospidéal Ollscoile Mater Misericordiae
Siúracha na Trócaire
Sráid Eccles, Baile Átha Cliath D07 R2WY, Éire

Tel: +353 1 8032000 Web: www.mater.ie

Not for prescription purposes

After Action Report – ICT Failure, 30th July 2024 at 11.46am

Failure Mode:

At 11:46am on the 30th of July 2024 the PatientCentre system that is central to the safe operation of the Hospital, presented with a data base application error. This was notified to the ICT team at 11:51am. At this point the ICT team commenced trouble shooting the [redacted] error. After several attempts to resolve the issue, a decision was made to escalate the problem to [redacted] as a P1 issue (Critical system failure – major incident).

[redacted] were notified at 13:02, and allocated an engineer at 13:18. The Hospital received all the requested support from [redacted] from the point of notification, until the issue was resolved under the existing Mater University Hospital service contract.

Section 33 - Security defence and international relations [redacted]

The failure of PatientCentre was caused due to the underlying legacy Operating System ([redacted] Section 33 - Security defence and international relations [redacted] When [redacted] encountered this issue it logged a [redacted] and prevented further updates to the [redacted] thus disabling PatientCentre.

Operational impact:

The Hospital is fully dependant on a number of critical systems to operate safe patient services in an efficient and effective manner. With the failure of PatientCentre all of the Hospitals processes that were managed and controlled electronically reverted to paper. The effect was an immediate impact on patient safety and the ability of the Hospital to track, plan and execute specific patient care requirements which will have had a negative impact on patient outcomes.

Section 33 - Security defence and international relations [redacted]

- Section 33 - Security defence and international relations [redacted]

Mater Misericordiae
University Hospital
Sisters of Mercy
Eccles Street, Dublin D07 R2WY, Ireland

Ospidéal Ollscoile
Mater Misericordiae
Siúracha na Trócaire
Sráid Eccles, Baile Átha Cliath D07 R2WY, Éire

Tel: +353 1 8032000 Web: www.mater.ie

Not for prescription purposes

Section 33 - Security defence and international relations

[redacted]

Mater Misericordiae
University Hospital
Sisters of Mercy
Eccles Street, Dublin D07 R2WY, Ireland

Ospidéal Ollscoile
Mater Misericordiae
Siúracha na Trócaire
Sráid Eccles, Baile Átha Cliath D07 R2WY, Éire

Tel: +353 1 8032000 Web: www.mater.ie

Section 33 - Security defence and international relations

[redacted]

Not for prescription purposes

History:

Section 29 - Deliberations of FOI bodies, Section 30 - Functions and negotiations of FOI bodies, Section 33 - Security defence and international relations

[redacted]

Not for prescription purposes

Mitigations for this Incident:

- The [redacted] was implemented in 2023 following discussion with the HSE. This allowed the teams to know who was due into the Hospital, who was in the Hospital and how to locate the paper chart and previous medical record number where available.
- All community Pathology requirement were outsourced to private labs.
- A number of Radiology Diagnostics were outsourced to private services.
- Radiology and Pathology ordering were moved to paper orders.
- 60 procedures including 32 surgical procedures were deferred. This included time sensitive urgent care. Support for outsourcing surgical activity in the private hospital system was denied by the HSE.
- All internal and external reports were unavailable, compromising and delaying informed decision making. Meeting 2-3 times per day to help with the distribution of critical information. Emails, phone calls and Silo was used to communication critical operational and clinical information. For example, no reporting was available on radiology, the consultants would call the referring clinical team if an urgent concern was identified.
- Contacted Healthlink to inform GPs that this pathway was not available. Despite this mitigation 420 GP referrals were made via health-link during the down time. Care for the 420 was delayed as a result of this failure.
- The Hospital had prior to this incident undertaken a table top exercise for ED to simulate a PatientCentre failure. From this the team had agreed a suite of documentation to support the services and the associated processes.
- A centralised document drive was deployed to support the manual recording needs of the service.
- Additional staff were deployed across the organisation to help move the paper orders, trace activity and support other manual activities. This is manageable for the period of the escalation, however it is not a sustainable solution for a period of failure that extends beyond 1-2 weeks.
- The Hospital purchased a corporate Siilo system to enable compliant communication between clinical and operational groups.
- The Hospital has emergency medical number to deploy when the system is down, enabling tracking of the patient through the Hospital. This does not mitigate and or consider the risk of lost documents, including medical files placing the patient at significant risk.

Please note this list is no exhaustive and will be updated with time

Technical Recovery:

- The Hospitals ICT team working with our external contracted party ([redacted] undertook the following activities to enable a system recovery,
- The Hospital team remained on the campus until 11pm on the night of the failure, working with [redacted] to identify the fault.
- The Hospital and [redacted] teams worked from 2pm on Tuesday the 30th of July until 9am Thursday the 1st of August to restore the system. At which point the teams commenced integrity checks which concluded at 8am on the morning of the 2nd August.
- Prior to going live (normal business) approximately 50 staff contributed to the technical and data recovery activities during the period of failure.
- Post go live, the Hospital continues to have data errors and omissions that necessitate additional admin support across the wider Hospital to bring the systems up to date. The clinical risk continues while the system has incomplete data.

Summary: Key Learnings

- Immediate Action: Quickly establish a separate MRN group and dedicated MRN issuing hub to manage emergency patient records.
- Support from Other Hospitals: Secure support from other hospitals to manage the initial transition to manual processes.
- Manual Census Importance: Implementing and maintaining a manual patient census is crucial for accurate patient tracking during downtimes.
- Outsourcing Diagnostics: Agree on outsourcing diagnostic services to manage urgent needs effectively.
- Communication: Timely and clear communication with the public and stakeholders is essential during system downtimes. Access to systems such as Vocera and Siilo are crucial to support rapid, confidential communication.
- Recovery Planning: Establish a dedicated upload centre and team to backload manual records efficiently once the system is restored. The time required for this task should not be underestimated.
- Risk Management: Define a 'good enough' handback point to balance the risk of manual system reliance.
- Operational Impact: Recognise and plan for the significant reduction in operational capacity, particularly in surgical procedures, diagnostic and laboratory procedures during extended downtimes.

Immediately Required Actions During Downtime:

- Vulnerability Period Management: Ensure immediate availability of a separate group of Medical Record Numbers (MRNs) to avoid duplicate MRNs during downtime.
- Dedicated MRN Hub: Establish a dedicated hub with increased staffing to issue new MRNs for emergency, in- and out-patients.
- Event Time Capture: It is crucial to record the time of patient-related events accurately. This was a gap in some documentation during this downtime.
- External Support: Request other Dublin hospitals to come off call for two hours to manage emergency service migration to manual processes, reducing pressure on the resuscitation area. Communicate within clinical groups and Patient Flow that inter-hospital transfers into MMUH will be restricted to critical transfers only.
- Smithfield Rapid Injury Unit: Close this Unit and reallocate staff to the main Emergency Department.
- Healthlink Referrals: Use direct log-on for Healthlink to prevent the loss of access to GP referrals. Backlogged referrals, despite requests to GPs to use other referral methods, totalled 420 during this downtime
- Pharmacy: All pharmacy activity reverts to full manual ordering, stocking and tracking
- Diagnostic ordering: All diagnostics are ordered manually. Radiology reporting is completed separately to NIMIS.

Actions Required for Downtime Exceeding Two Hours:

- Operational Steering Meeting: Convene an urgent meeting with executive and clinical stakeholders to outline mitigations, identify risk areas, and review activities for the next 24 hours, including deferral agreements.

- Outsourcing: Agree on outsourcing radiology and laboratory services to meet urgent diagnostic needs.
- Public Communication: Issue media communications about situation and expected delays for non-urgent attendances.
- Manual Patient Census: Implement a manual census using Excel templates for accurate tracking of patient admissions, discharges, and transfers.
- Additional Staffing: Deploy extra administrative staff to support manual tasks in ED registration, admissions, patient flow, and medical records, as well as portering staff for request transfers.

Recovery Period:

- Dedicated Upload Centre: Establish a centre with 10-15 terminals and a specialised team to backload manual records once the system is restored for specific users.
- Team Composition: The team should include medical records, registration, admissions, experienced ward clerks, and information management specialists.
- Sequence for Backloading Records before Handback:
- ED patients (awaiting admission and at ED level of care)
- Inpatients discharged during downtime
- Inpatients transferred during downtime
- Inpatients admitted during downtime
- Registered day cases on system return day
- Emergency-treated patients subsequently discharged
- Handback Agreement: Determine a 'good enough' handback point to minimise risks from prolonged reliance on manual systems. The dynamic nature of patient care means a gap between real-time and handover will exist, but can be corrected locally once the system is running for all users.

Post-System Handback:

- Further Back loading Required:
  - Outpatient attendances and future bookings
  - Future procedures and referrals
  - Day case activities
  - Theatre activities
  - Other order activities (e.g., health and social care)

It needs to be noted, at this point (6.08.2024) the teams are still working to load documents related to the manual work.

One of the last aspects of the PatientCentre restore was executed on the morning of 7th August 2024 which involved re-invoking the Dayend process (this is the process that automatically manages patient Did Not Attends, Clinic roll ons and IP Waiting List Management). At this point we have 3,000+ Outpatient appointments and 700+ Diagnostic/Service appointments that will be marked as Did Not Attends as the user had no ability to register those patients on the day. The patient record will show DNA despite the patient attending the Hospital for their appointment or procedure. A backdated registration is on file to capture the action and the procedure may have been resulted. This duplication will create some issues with external communication in the form of inaccurate data and communications to GPs, limited to the files effected during this period. It should also be noted that DNA notifications are sent to some of our downstream systems including Healthlink and NTPF.

Not for prescription purposes

General Operational Comments:

- Patient Impact: 60 procedures were deferred to ensure safe patient transit through theatre during manual system use.
- Staffing Needs: Additional staffing was required but only sustainable for 4 days of downtime. Longer outages will require adjusted rotas, outsourcing and overtime as well as decreased activity to sustain safe practice
- Back loading Duration: Inpatient and ED back loading took two working days, while outpatient and discharged ED patient back loading could take a week with overtime.
- Contingency Plans: Read-only templates for commonly used documents should be available at all terminals, with hard copies as backups. Hardcopy order forms for all diagnostics should be available in each clinical area.
- Data Extract Issues: Notify stakeholders about erroneous or missing data extracts and delayed reports due to reliance on PatientCentre for external reporting.
- Operational Capacity Impact: Downtime significantly impacted surgical access, with a 30%-50% reduction in procedure capacity for downtimes over 24 hours.
- Outpatient Clinics: Clinics ran at capacity initially but would have faced up to a 50% reduction by the second week of downtime.

Mater Misericordiae University Hospital
Sisters of Mercy
Eccles Street, Dublin D07 R2WY, Ireland

Ospidéal Ollscoile Mater Misericordiae
Siúracha na Trócaire
Sráid Eccles, Baile Átha Cliath D07 R2WY, Éire

Tel: +353 1 8032000 Web: www.mater.ie

Not for prescription purposes

Policy

[redacted]

Summary

The risk of a catastrophic technical failure of PatientCentre at the Mater Hospital needs to be addressed urgently. A number of the critical elements of the system are well beyond end of life and are not supported and have no options in relation to the provision of technical support. [redacted]

Services were effected for the entirety of the outage, this included an unknown level of harm to the patients. No assurance can be given that system will not fail at any point into the future. Furthermore, if the failure is in one of the unsupported elements of the system the failure may be unrecoverable.

As the Hospital delivers approximately €560m in acute adult services, a reduction in activity will result in up to €280m is opportunity losses (service loss) in the first 12 months if a 50% loss is realised. It also needs to be noted that the time to install a solution is 18-24 months, pushing that loss up significantly.

A technical failure that results in the loss of PatientCentre will impact all the Hospital services including the 17 National services provided at the Mater Hospital. The Hospitals capacity to deliver safe and efficient services will be diminished immensely increasing risk to patients who can access care at the Hospital.

[redacted]

Not for prescription purposes

[redacted]

The Hospital have formed a view that the Regional solution will take at least 4-7 years given both scale and complexity of the solution being envisaged. The Hospital acknowledges that we will need to manage risk for 18-24 months if approval is granted to the MMUH, however this is significantly less that the expected time for the regional system. For this reason waiting for the regional solution is not an option that the Hospital can support.

Last week we had an insight into the chaos caused by a technical failure that lasted less than 5 days. The frequency of failures has grown in the past 12 months which is a concern, the only option now is the solution proposed in 2021, again in 2022 and again in 2023, to approve the MMUH EHR without further delay.

Interim Solution

[redacted]

Root Cause Analysis Report for the Mater Misericordiae University Hospital (Mater) - Section 33 - Security defence and international relations

Date: 14th August 2024

Section 33 - Security defence and international relations

[redacted]

[redacted]

[redacted]

Table of Contents

[redacted]

Executive Summary

Brief Description of Incident

Mater Misericordiae University Hospital ("Mater"), experienced a multi-day outage of its mission-critical PatientCentre EHR resulting from a failed [redacted] expansion.

Incident Date/Time

30 July 2024 11:51 (Incident occurred).

30 July 2024 13:02 (Incident reported).

01 Aug 2024 14:13 (Incident reported as resolved with restricted access for users).

Impact on Service

Unable to access Patients' Electronic Health Records which impacted patient care and safety.

Summary of Root Causes

We can conclude that the failure was caused by mismatch occurring between the operating system ([redacted]), and the [redacted] platform during a manual [redacted] expansion.

Due to the impact on operations, the decision was taken during the event to prioritize recovery over investigation. Consequently, the root cause cannot be definitively established as sufficient evidence was not collected at the time of incident.

Once the failure was detected, the [redacted] platform paused further updates to prevent any [redacted] degradation, which helped to recover 100% of data without any loss.

Section 33 - Security defence and international relations [redacted]

[redacted]

Evidence

[redacted] shows the initial sequence of a [redacted] expansion followed by an error writing to the [redacted] Then after five minutes (301 seconds), it shows [redacted] performing a designed pause to prevent further damage.

- 07/30/24-11:50:49:534 Section 33 [redacted] - Securi [redacted] defence [redacted]
- 07/30/24-11:56:16:239 Section 33 - Security defence and international relations [redacted]

[redacted] analysis shows an error being returned from [redacted] which can be interpreted as an attempt to write past the end of a file: [redacted]

[redacted]

Root Causes

The evidence shows that [redacted] and [redacted] disagree on the file size, and this occurs immediately following a [redacted] file expansion operation. It also shows that the [redacted] file being operated on is fragmented, though not severely so, at the [redacted] level. We believe the failure occurred when [redacted] tried to update the [redacted] at a location [redacted] believe was beyond the end of the file.

With the available evidence, it is not possible to determine how the discrepancy in file size between [redacted] and [redacted] occurred.

[redacted]

Recommendations

Due to the extreme legacy hardware and Operating System configuration, [redacted]. Section 33 - Security defence and international relations [redacted]

[redacted]

[redacted] Section 36 - Commercially sensitive information, Section 33 - Security defence and international relations [redacted]

Therefore, given the challenges and significant risks associated with maintaining PatientCentre, it is recommended that the Mater seriously consider the replacement of PatientCentre as a matter of urgency.

In the interim period, access to PatientCentre and the data within PatientCentre, should be considered at high risk and the Mater should ensure that it has adequate risk mitigation strategies in place in case of system failure or a data breech.

Before undertaking [redacted] expansions or other similar system maintenance functions, it is recommended to contact [redacted] for advice to ensure that associated operational risks are minimised.

Note: Section 33 - Security defence and international relations [redacted]

[redacted]

Section 33 - Security defence and international relations

[redacted]