INF20031

BCM Report

By: Zoe Bobinac 103644760,

Kelly Hung 104084451,

Erika Ignatius 104286532,

Tran Anh Thu Pham 103818400

Due Date: 18/10/2024

Executive Summary

Business Continuity Management (BCM) is critical to Bayview Regional Health Centre (BRHC) in ensuring the uninterrupted delivery of essential healthcare services during disruptions. Given BRHC has reliance on digital systems and its role in safeguarding patient care, a strong BCM framework is essential to mitigate risks associated with cyberattacks, system failures, or natural disasters. The following report highlights the importance of BCM, key recommendations for improving information governance, and the essential components of an Enterprise Information Security Policy (EISP), aligning with BRHC's overall strategic objectives.

Key Findings and Recommendations:

Importance of BCM: BCM at BRHC is vital to protect patient care, sustain stakeholder trust, and comply with healthcare regulations. In the event of disruptions, BCM enables rapid recovery, minimising operational downtime and maintaining critical healthcare services.

Information Governance: To improve information governance, BRHC should adopt centralised data management systems and role-based access control (RBAC) to streamline data flow and enhance security. Additionally, regular audits and compliance checks will ensure adherence to regulations and data integrity, while cross-departmental data-sharing platforms will ensure timely access to crucial information.

Enterprise Information Security Policy (EISP): BRHC should develop a comprehensive EISP that incorporates security frameworks like ISO 27001, outlining policies for data protection and incident response. Real-time threat detection systems, continuous staff training on cybersecurity, and automated monitoring tools are recommended to secure patient data and prevent breaches.

Business Impact Assessment (BIA): Critical systems at BRHC, such as the Electronic Health Records (EHR), Patient Scheduling, Laboratory Information Management (LIMS), and Pharmacy Management Systems, are essential for ensuring continuity in patient care. These systems must be prioritised for immediate recovery in the event of disruptions, with detailed recovery objectives and risk assessments for each system.

Disruption Scenarios: Two major disruption scenarios were assessed: a ransomware attack on patient records and a LIMS failure. In both cases, the objectives are to restore functionality within the shortest timeframes, ensuring minimal impact on patient care and regulatory compliance.

Implementing the recommendations for BCM, information governance, and EISP will position BRHC to respond effectively to future disruptions while maintaining the highest standards of healthcare service delivery. By prioritising system recovery and securing information assets, BRHC can enhance resilience, protect patient safety, and sustain trust.

Table of Contents

Scope and Purpose of Business Continuity Management (BCM) at Bayview Regional Health Centre

a) A strategic overview of the importance of BCM at Bayview Regional Health Centre.

Business Continuity Management (BCM) is essential for Bayview Regional Health Centre (BRHC) to ensure that critical healthcare services remain operational during disruptions. Given that BRHC provides vital healthcare services, the continuity of operations is paramount to safeguarding patient care, maintaining stakeholder trust, and meeting regulatory obligations. BCM ensures that BRHC can quickly recover from unforeseen events such as cyberattacks, natural disasters, or system failures, minimising disruptions and maintaining the availability of critical medical services.

b) Key recommendations for improving information governance across the centre's value chain.

Centralised Data Management: Implement a centralised data management system that integrates all departments to ensure real-time access to critical information. This will enhance data consistency and streamline decision-making. (El aboudi & Benhlima, 2018)

Role-Based Access Control (RBAC): Establish RBAC policies to ensure that sensitive information is accessed only by authorized personnel, reducing the risk of data breaches and non-compliance. (ISO/IEC 27001)

Regular Audits and Compliance Checks: Conduct routine audits across the information governance lifecycle to ensure compliance with internal policies and external regulations, as part of the cybersecurity audit and assurance processes. (NIST 800-30) (ISO 31000)

Data Integrity and Backup Solutions: Implement robust data backup and integrity verification processes to ensure that, in the event of a disruption, accurate and up-to-date information is available to continue operations. (ISO 27001) (NIST 800 - 53)

To make departmental data sharing more efficient, use middleware or data integration platforms. This will guarantee that correct and current information is available to all pertinent departments. SOPs should be created for data entry, sharing, and reporting to reduce errors and discrepancies during data flow. Adopt and promote the adoption of common standards for data interchange to increase communication between different health information systems.

To make sure that high-quality data is maintained, conduct regular audits to verify the correctness and completeness of the data and to quickly fix any errors. Staff members should get training on the value of data integrity and appropriate data management techniques. Use automated technologies for data quality that can verify and clean data before it is entered into the system.

Create thorough information governance policies that address security, privacy, and adherence to laws and regulations. Review and update these policies regularly. Establish a compliance monitoring program to verify adherence to regulatory obligations and corporate regulations. Using automated compliance technologies to monitor and report on compliance status may fall under this category. Establish a simple and easy-to-use system for reporting governance or data breach incidents. Ensure that there is an established method for responding to such situations.

To manage information governance tasks and handle cross-functional difficulties, organise a governance committee of representatives from all important departments. Organise frequent training sessions to inform employees of the value of information governance and their roles in its upkeep.

c) Key recommendations for an Enterprise Information Security Policy (EISP) for BRHC.

Comprehensive Security Framework: Design an Enterprise Information Security Policy (EISP) that aligns with industry standards such as ISO 27001 or NIST, focusing on the protection of patient data and the confidentiality, integrity, and availability of information systems.

Incident Response Plan: Incorporate a well-documented incident response plan into the EISP, detailing how BRHC should react to data breaches, cyberattacks, and system outages to mitigate damages quickly and restore services. (NIST 800-61)

Training and Awareness Programs: Regularly train staff on information security practices and updates to the EISP, ensuring that all personnel understand their role in safeguarding critical assets. (ISO 27001)

Continuous Monitoring and Threat Detection: Implement tools for continuous monitoring of the network, along with a Security Information and Event Management (SIEM) system to detect and respond to security incidents in real time. (González-Granadillo et.al., 2021).

d) The significance of information governance and the EISP in maintaining business continuity for BRHC.

Information governance and an EISP are cornerstones in maintaining business continuity at BRHC. Effective governance ensures that accurate, up-to-date information is available, which is vital for clinical decision-making during emergencies. (Information and Cyber Security Governance, Risk and Compliance (GRC), 2023) Without proper governance, data silos, outdated information, or unauthorised access could disrupt operations, endanger patient safety, and erode trust. The EISP, on the other hand, serves as a blueprint for securing BRHC's digital assets, outlining procedures for handling data breaches, maintaining system integrity, and recovering from cyber incidents. (RSI Security, 2019) Together, these

frameworks ensure that BRHC can continue its operations uninterrupted, even in the face of disruptive events. (ISO 27001)

Business Impact Assessment

a) Prioritise systems within BRHC for a business impact assessment

The table below shows detailed prioritise systems along with business units within BRHC for a business impact assessment:

System name	Functionality Description	Business Units	Priority level (1-4)
Electronic health records (EHR) system	- Stores patient medical histories, diagnoses, and treatment plans. - Maintains laboratory and test results. - Provides a central source of patient data for healthcare providers. - Ensures timely and accurate medical care.	Clinical Services, IT, Medical Records	4 (Critical)
Patient scheduling system	- Manages patient appointments. - Allocates resources for clinical workflow optimization. - Minimizes patient wait times. - Optimizes staff and medical resources scheduling.	Administration, Clinical Services, IT	4 (Critical)

Laboratory Information Management System (LIMS)	- Manages laboratory workflows. - Processes test orders and results. - Ensures timely and accurate diagnostics. - Manages inventory and laboratory supplies.	Laboratory, IT, Clinical Services	4 (Critical)
Pharmacy management system	- Controls medication inventory. - Manages prescription orders and drug dispensing. - Ensures patient safety and compliance with pharmaceutical regulations. - Prevents medication errors and stock shortages.	Pharmacy, Clinical Services, IT	4 (Critical)
Medilink system	- Manages patient records and scheduling. - Handles billing and administrative functions. - Ensures streamlined communication between departments. - Supports regulatory compliance and financial management.	Administration, Medical Records, IT	3 (High)

Telehealth System	- Provides remote healthcare consultations and diagnostics. - Extends services to patients in distant or rural areas. - Enables patient management and monitoring remotely. - Ensures continuity of care for non-local patients.	Telehealth, Clinical Services, IT, Administration	1 (low)
Medical Imaging System (PACS/RIS)	- Stores and retrieves medical images (X-rays, MRIs, CT scans). - Share diagnostic images with healthcare providers. - Facilitates diagnosis and treatment planning. - Enhances collaboration between radiologists and physicians.	Radiology, Clinical Services, IT	2 (Medium)

- **Electronic health records (EHR) system:** The EHR system is essential for organising and keeping track of patient medical data. It acts as the main database for patient information, containing diagnosis results, treatment plans, and medical history. This system is a high-priority asset for BIA since it contains sensitive data that is essential to patient care and legal compliance. (Health, 2021)
- **Patient scheduling system:** To minimise wait times, guarantee effective resource usage, and manage patient appointments, this system is crucial. For both operational effectiveness and patient pleasure, scheduling must be done well. Interruptions in this system may result in a backlog of patients and lower-quality service.

- **Laboratory Information Management System (LIMS)**: Laboratory test orders, results, and supply inventory are all managed using LIMS. It is important for making judgments about diagnosis and therapy. For the sake of patient care, quick and accurate test findings are essential. If there is a disruption in this system, patient outcomes may suffer from delayed diagnoses and treatments. (Yesford, 2023)
- **Pharmacy management system:** Prescription management, drug inventory tracking, and medicine delivery are all under the control of the pharmacy management system. Any disruption to this system could have major effects on patient health because it is essential for guaranteeing patient safety and legal compliance with pharmaceutical rules.
- **Medilink System:** a high-priority system that integrates patient record management, scheduling, billing, and administrative functions. It supports crucial aspects of healthcare delivery by ensuring smooth communication between departments, patient data management, and regulatory compliance. Any interruption could severely disrupt clinical operations and financial management, affecting patient care and billing processes.
- **Telehealth system**: facilitates remote consultations and diagnostics, enabling healthcare delivery to patients in rural or distant locations. Though not critical for immediate hospital operations, its importance in extending care beyond physical borders is significant, especially for non-local patients. Disruptions could limit access to care for remote patients but would not affect on-site operations.
- **Medical Imaging System (PACS/RIS)**: manages the storage and retrieval of diagnostic medical images, such as X-rays, MRIs, and CT scans, and facilitates collaboration between radiologists and physicians. It is vital for diagnosis and

treatment planning, and its disruption could lead to delayed diagnoses and compromised patient care.

b) Four priority areas and explain their importance for BIA

In conducting a Business Impact Assessment (BIA) for Bayview Regional Health Centre (BRHC), we prioritise four critical priority areas. These areas are essential for maintaining continuity in patient care, ensuring legal compliance, and safeguarding critical information assets:

- **Electronic Health Records (EHR) System:** The EHR system is central to BRHC's healthcare operations, storing patient medical histories, diagnoses, and treatment plans. As the main source of patient data, any disruption would severely impact timely and accurate care. EHRs also contain sensitive information, crucial for compliance with privacy regulations. If the system goes down, the hospital's ability to provide care would be compromised within hours, affecting most clinical services. Therefore, it is the highest-priority system. (HealthIT, 2008)
- **Patient Scheduling System:** manages appointments, resource allocation, and clinical workflows. Its efficient operation minimizes patient wait times and optimizes staff and resource use. A failure could lead to delays, overcrowding, and patient dissatisfaction, affecting care quality and operational efficiency. Disruption would cause cascading delays, decreased productivity, and harm the hospital's reputation. Given its impact on workflow and patient satisfaction, it is considered a critical system. (goodx.healthcare, 2024)
- **Laboratory Information Management System (LIMS)**: manages test orders, results, and laboratory workflows, essential for diagnosis and treatment decisions. A disruption could delay test results, risking misdiagnoses or delayed treatments. LIMS

also manages inventory, ensuring critical supplies are available. Given its role in timely diagnoses and treatment, LIMS is a top priority. Delays in results could be life-threatening for urgent cases, and prolonged outages could deplete essential lab supplies, further impacting patient care. (Illumina, 2024)

- **Pharmacy Management System:** controls medication inventory, prescription orders, and drug dispensing. Maintaining an accurate system is vital for patient safety and compliance with pharmaceutical regulations. Disruptions could lead to medication errors, stock shortages, or overdoses, adversely affecting patient safety and BRHC's legal compliance. Given that medication errors are a leading cause of patient harm, the pharmacy system is essential for healthcare delivery. Its significant impact on patient safety and regulatory compliance underscores its critical status. (AltexSoft, 2021)

c) Detailed BIA for top four prioritised areas

The table below is a detailed Business Impact Assessment (BIA) for the four identified prioritised areas at Bayview Regional Health Centre (BRHC):

Priority Area	Critical Business Function	Information Assets / Critical IT System at Risk	Business Impact	Overall Impact Level	MTD/MAO (Maximum Allowable Downtime)	RTO (Recovery Time Objective)
Electronic Health Records (EHR) System	Delivering Patient Care Services	Patient medical history, treatment plans, diagnoses	- Severe delays in providing care, potential misdiagnoses, and treatment interruptions - Legal and regulatory implications related to privacy breaches	**Consequence:** High **Likelihood:** Medium **Risk Rating:** High **Impact Level:** Critical	12 hours	4 hours
Patient Scheduling	Scheduling and	Appointment data,	Patients could miss appointments, clinic	**Consequence:** Medium	24 hours	6 hours

System	Managing Appointments	staffing schedules, resource allocation	inefficiencies, and reputational damage due to delayed or cancelled appointments	**Likelihood:** Medium **Risk Rating:** High **Impact** Level: High		
Laboratory Information Management System (LIMS)	Diagnostic Services (Laboratory Operations)	Lab test results, inventory management, diagnostic data	Delays in obtaining lab test results, affect treatment decisions and overall patient outcomes	**Consequence:** High - Likelihood: Medium - Risk Rating: High - Impact Level: Critical	24 hours	8 hours
Pharmacy Management System	Managing Medication and Prescriptions	Prescription records, medication inventory, patient drug information	Disruption in medication delivery, leading to risks of incorrect dosages, patient safety concerns, and inventory mismanagement	**Consequence**: High **Likelihood:** Medium **Risk Rating:** High **Impact:** Critical	12 hours	4 hours

- **Electronic Health Records (EHR) System:** is essential for patient care at BRHC, storing crucial medical information like histories, diagnoses, and treatment plans. A failure would have high consequences due to its immediate impact on patient safety, care continuity, and regulatory compliance. Delays in accessing EHR can hinder timely treatments or lead to diagnostic errors, severely affecting patients. The likelihood of failure is medium, thanks to safeguards and backup measures; however, external threats like cyberattacks remain a risk. Given the potential severity of consequences, the risk rating is high, and the overall impact level is critical. BRHC has set a maximum allowable downtime (MTD) of 12 hours, allowing this duration of downtime before care is critically compromised. The recovery time objective (RTO) is 4 hours, emphasizing the need for swift restoration to minimize disruption. (Tracie, 2015)

- **Patient Scheduling System:** is vital for managing appointments and staff resources at BRHC. The consequences of a failure are rated medium, as disruptions could result in missed or delayed appointments, causing inefficiencies and reputational damage, but not posing an immediate threat to patient safety. The likelihood of failure is also medium, with technical issues or human errors leading to temporary downtime, though preventive measures minimize long-term disruptions. The risk rating is high, as inefficiencies can significantly impact hospital functions over time, despite being less severe than EHR-related issues. The overall impact level is high since patient care could be indirectly affected by scheduling problems. BRHC has established a maximum allowable downtime (MTD) of 24 hours, allowing one day of disruptions before facing serious challenges. The recovery time objective (RTO) is set at 6 hours to ensure swift recovery and minimize effects on clinic schedules and patient satisfaction. (goodx.healthcare, 2024)
- **Laboratory Information Management System (LIMS):** is vital for managing diagnostic services, including lab test results, inventory, and diagnostic data. The consequences of a failure are high, as delayed lab results can hinder clinicians' ability to make informed treatment decisions, worsening patient outcomes, especially in urgent cases. Additionally, inventory mismanagement could lead to stock shortages, complicating the situation. The likelihood of a LIMS failure is medium due to the complexity of operations and external threats like hardware or software issues. Given the critical importance of lab results in treatment, the risk rating is high, and the overall impact level is critical. BRHC has set a maximum allowable downtime of 24 hours, allowing one day of disruption before patient outcomes are severely compromised. However, the recovery time objective (RTO) is 8 hours, emphasizing the need for rapid recovery to avoid prolonged delays. (Illumina, 2024)

- **Pharmacy Management System:** ensures patients receive the correct medications and dosages. The consequences of a failure are high, as prescription errors or delays in dispensing medications pose serious risks to patient safety. Additionally, inventory management failures may lead to medication shortages, compromising care. The likelihood of system failure is medium due to vulnerabilities to technical issues and cyber threats, despite existing security measures. Given its direct impact on patient safety, the risk rating is high, and the overall impact level is critical. BRHC has established a maximum allowable downtime of 12 hours, after which patient safety could be compromised if medications are not delivered on time. The recovery time objective (RTO) is set at 4 hours, emphasizing the need for swift recovery to prevent serious errors and ensure continuity in patient care. (AltexSoft, 2021)

d) Two Major Disruption Scenarios, Objectives and Parameters

Scenario 1: Ransomware Attack on Patient Records

A ransomware attack would lock access to BRHC's Electronic Health Records (EHR) system, making patient records unavailable for up to six weeks. This would significantly disrupt patient care, delay treatment decisions, and cause potential legal non-compliance due to privacy and data security regulations (Privacy Act 1988, 2024).

Recovery Objective: Restore access to the EHR system and patient records within 2 weeks using backup data and paper-based/manual methods to ensure continuity of care. Full system restoration would ideally occur within 4-6 weeks (Sittig, & Singh, 2016).

Parameters: Prioritise data recovery and patient safety by ensuring backups are secure, tested, and accessible (Beaman et al, 2021). Temporary paper-based workflows and communication with external specialists will be vital to mitigate delays in critical care decisions.

Scenario 2: Laboratory Information Management System (LIMS) Failure

A failure in the LIMS disrupts diagnostic testing and results, impacting decision-making for treatment. It affects patient care quality and causes delays in medication administration and surgical procedures reliant on test results.

Recovery Objective: Ensure the LIMS is restored and functional within ideally 24 hours, with priority given to critical tests (emergency and surgery-related) through manual processes.

Parameters: Enable lab technicians to manually process high-priority tests while IT restores system access, ensuring that manual documentation can be securely integrated into the system post-recovery.

Incident Response Planning

a) Incident Response Handling Plans

Ransomware Incident Response Plan: See Appendix A for a comprehensive list.

- **Before**: Train users to avoid suspicious files and ensure antivirus software is up to date across all systems.
- **During**: Disconnect infected systems from the network, notify IT immediately, and begin scanning for the ransomware strain.
- **After**: Conduct recovery investigations, reconnect quarantined systems, and update all users on the status of antivirus and malware definitions.

LIMS Failure Incident Response Plan: See Appendix B for a comprehensive list.

Before: Ensure system backups are in place and staff are trained on manual workflows in case of system downtime.

During: Switch to manual processes for lab management, notify IT, and escalate issues affecting patient care to leadership.

After: Investigate the root cause, restore normal system functions, and brief staff on the incident and prevention measures.

b) Crisis Communications Plan

Internal Communication: Immediately notify BRHC leadership, staff, and key departments such as clinical, IT, and legal about the disruption (Marsen, 2020). Provide clear instructions for interim procedures such as manual workflows. An example would be: "Attention all staff, we have detected a ransomware attack that is affecting our IT systems. IT and cybersecurity teams are currently addressing the issue. Please follow the manual protocols for clinical workflows as outlined in your department procedures until further notice. Do not attempt to use your computer or log into the network until IT services provide further instructions. We are working to resolve this as swiftly as possible. Further updates will be provided regularly."

External Communication: Inform patients, regulatory authorities, and the public about service disruptions, ensuring transparency about the issue, timelines for recovery, and alternative care arrangements. For example: "We are facing a serious ransomware attack that has temporarily disrupted our operations. I want to assure you that we are working around the clock to contain the breach and restore services. In the meantime, it’s crucial to stick to manual processes and stay vigilant. We appreciate your cooperation and will provide frequent updates."

Media Management: To manage the narrative, choose a spokesperson and create a message that emphasises BRHC's dedication to patient safety and the actions taken to address the disruption (Safitra et al, 2023). It might be "BRHC is currently experiencing technical

difficulties due to a cyberattack. We want to assure our patients that we are implementing contingency plans to ensure their care continues with minimal disruption. We are working with cybersecurity experts and expect to restore normal services shortly. Patients may experience slight delays, but we are doing everything possible to maintain high-quality care. For urgent care, our emergency services remain fully operational."

Updates and Follow-ups: Provide regular updates on recovery progress to all stakeholders, including any changes in timelines or procedures. After recovery, share a comprehensive report detailing the incident and improvements made to prevent future disruptions.

References

Beaman, C., Barkworth, A., Akande, T. D., Hakak, S., & Khan, M. K. (2021). Ransomware: Recent advances, analysis, challenges and future research directions. *Computers & security*, *111*, 102490. https://doi.org/10.1016/j.cose.2021.102490

El aboudi, N., & Benhlima, L. (2018). *Big Data Management for Healthcare Systems: Architecture, Requirements, and Implementation*. *Advances in Bioinformatics*, 2018, Article ID 4059018, 1-10. https://onlinelibrary.wiley.com/doi/pdf/10.1155/2018/4059018

González-Granadillo, G., González-Zarzosa, S., & Diaz, R. (2021). *Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. Sensors, 21*(14), 4759. https://www.mdpi.com/1424-8220/21/14/4759

ISO/IEC 27001 *International Organization for Standardization. (2013). ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements. ISO.*

ISO 31000 International Organization for Standardization. (2018). *ISO 31000:2018 Risk management — Guidelines. ISO.*

Marsen, S. (2020). Navigating Crisis: The Role of Communication in Organisational Crisis. International Journal of Business Communication, 57(2), 163-175. https://doi.org/10.1177/2329488419882981

NIST 800-30 National Institute of Standards and Technology. (2012). *NIST Special Publication 800-30: Guide for conducting risk assessments. U.S. Department of Commerce.* https://doi.org/10.6028/NIST.SP.800-30r1

NIST 800-53 National Institute of Standards and Technology. (2020). *NIST Special Publication 800-53: Security and privacy controls for information systems and organizations. U.S. Department of Commerce*. https://doi.org/10.6028/NIST.SP.800-53r5

NIST 800-61 National Institute of Standards and Technology. (2012). *NIST Special Publication 800-61: Computer security incident handling guide. U.S. Department of Commerce.* https://doi.org/10.6028/NIST.SP.800-61r2

Privacy Act 1988. (2024). *The Privacy Act 1988: An overview*. Office of the Australian Information Commissioner. https://www.oaic.gov.au/privacy/privacy-legislation/the-privacy-act

Safitra MF, Lubis M, Fakhrurroja H. (2023). Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity. *Sustainability*. 15(18):13369. https://doi.org/10.3390/su151813369

Sittig, D. F., & Singh, H. (2016). A Socio-Technical Approach to Preventing, Mitigating, and Recovering from Ransomware Attacks. *Applied clinical informatics*, *7*(2), 624–632. https://doi.org/10.4338/ACI-2016-04-SOA-0064

Yesford, S. (2023, November). What is a LIMS And Why Do You Need One? The Connected Lab; Thermo Fisher Scientific. https://www.thermofisher.com/blog/connectedlab/what-is-a-lims/

Information and Cyber Security Governance, Risk and Compliance (GRC). (2023). Pluralsight.com. https://www.pluralsight.com/courses/governance-risk-compliance-information-cyber-security?clickid=1230027e66441599b4006575ef8df60e&utm_source=bing&utm_medium=paid-search&utm_campaign=upskilling-and-reskilling&utm_term=ssi-apac-bing-dynamic&utm_content=free-trial&msclkid=1230027e66441599b4006575ef8df60e

RSI Security. (2019, April 5). What Is The Purpose Of An Enterprise Information Security Policy? RSI Security. https://blog.rsisecurity.com/what-is-the-purpose-of-an-enterprise-information-security-policy/

Health. (2021, December 7). Electronic health records. Australian Government Department of Health and Aged Care. https://www.health.gov.au/topics/health-technologies-and-digital-health/about/electronic-health-records#:~:text=Electronic%20health%20records%20store%20your%20health%20information%20in,health%20records%20to%20help%20plan%20your%20ongoing%20care.

Electronic health records and downtime procedures. (2015, September 15). ASPR TRACIE. https://asprtracie.hhs.gov/technical-resources/resource/12142/electronic-health-records-and-downtime-procedures

What are the advantages of electronic health records? | HealthIT.gov. (n.d.). https://www.healthit.gov/faq/what-are-advantages-electronic-health-records

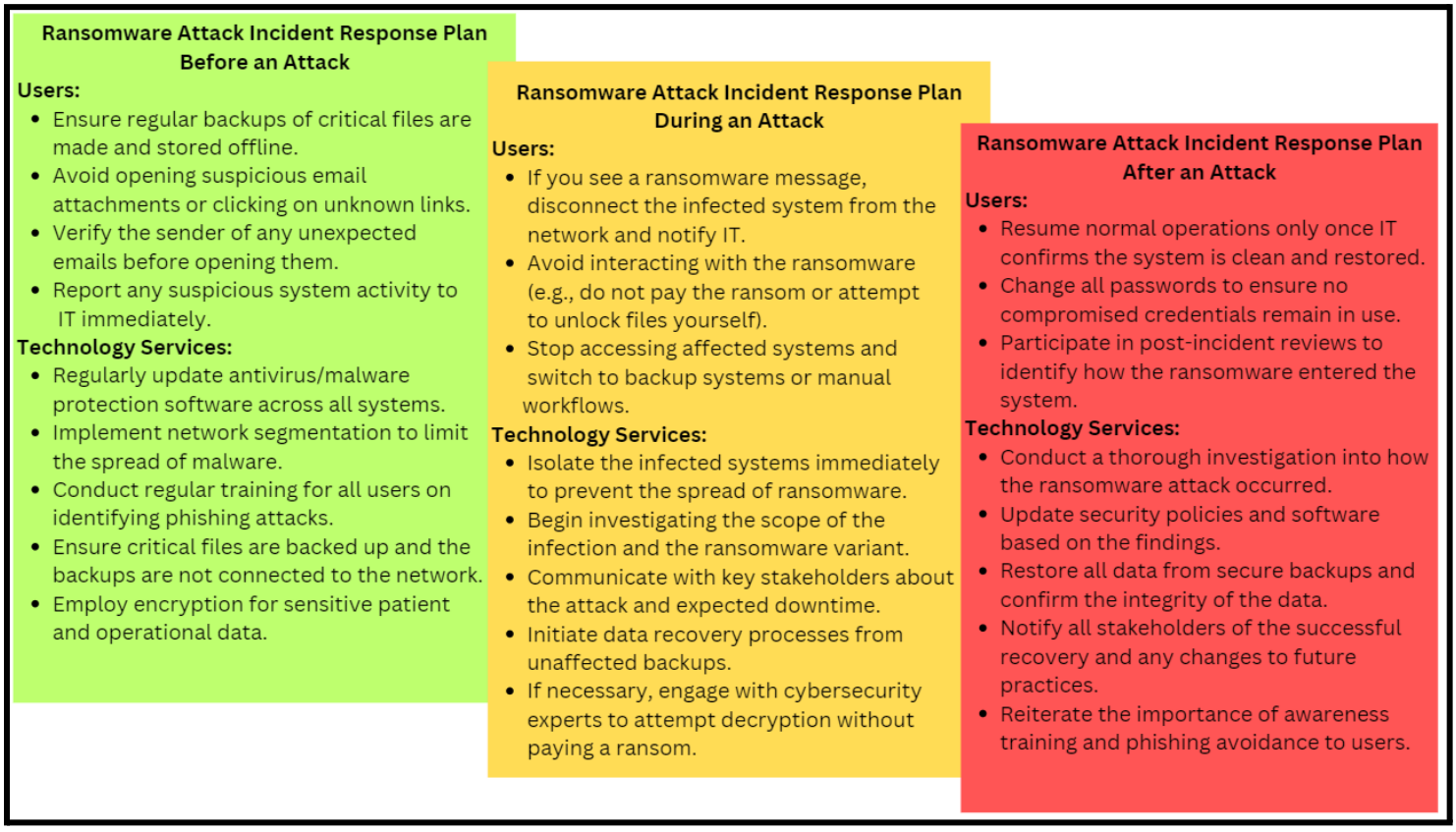
Laboratory information management systems (LIMS). (n.d.). Illumina | Sequencing and array-based solutions for genetic research. https://sapac.illumina.com/informatics/infrastructure-pipeline-setup/lims.

Editor. (2021, 13). Pharmacy management system: Benefits, features, providers. AltexSoft. https://www.altexsoft.com/blog/pharmacy-management-system/

One moment, please... (n.d.). One moment, please... https://www.goodx.healthcare/news/the-importance-of-patient-scheduling-in-a-healthcare-practice/

Appendices

Appendix A - Comprehensive Ransomware Attack Incident Response Plan



Appendix B - Comprehensive LIMS Attack Incident Response Plan