7COM1066-0901-2024

Information Security, Management and Compliance

ID:20049583
NOVEMBER 2024

Table of Contents

1. Organizational Context....3

2. Basic Criteria....3

2.1. Risk Management Approach....3

2.2. Risk Evaluation Criteria....4

2.3. Impact Criteria....4

2.3. Risk Acceptance Criteria....4

3. Scope and Boundaries....5

4. Organization and Responsibilities....5

3.Protection of Records Policy for Synnovis....7

3.1 Purpose....7

3.2 Scope....7

3.3 Access Control....7

3.4 Data Management....8

Evaluation and Approach in regard to using an AI tool (ChatGPT in my case)....11

Appendix 1: 13

Fig A: Images from Synnovis Booklet....13

Table A: Table provided in Unit 6....17

1. Organizational Context

Purpose and Objectives: Synnovis, a partnership between SYNLAB and NHS Trusts (Guy's and St Thomas' and King's College Hospital), operates as a pathology and diagnostic services provider, serving southeast London. The organization aims to deliver high-quality laboratory services to support the NHS Long-Term Plan's goal for integrated healthcare delivery. (Appendix 1 Fig A)

Legal and Regulatory Framework: As Synnovis processes and stores significant amounts of patient data, it adheres strictly to GDPR requirements, particularly concerning data minimization, purpose limitation, and consent management. Synnovis follows ISO/IEC 27001 standards to establish, implement, maintain, and continually improve its information security management system (ISMS), ensuring the confidentiality, integrity, and availability of information assets.

Stakeholders:

- **NHS Trusts**: Partner organizations, including Guy's and St Thomas 'NHS Foundation Trust and King's College Hospital, rely on Synnovis for pathology services, influencing service standards, regulatory compliance, and data security requirements.(Appendix 1 Fig A)
- **Patients**: Individuals receiving diagnostic services from Synnovis rely on accurate and timely test results for medical care decisions.
- **SYNLAB Network**: As a co-owner and operational partner, SYNLAB oversees business operations(Appendix 1 Fig A)
- **Internal Staff**: Employees involved in clinical, administrative, and IT roles who manage, process, and secure sensitive patient data as part of Synnovis's operational framework.

2. Basic Criteria

2.1. Risk Management Approach

Risk management approach consists of further steps which include.

Risk Identification: Synnovis identifies risks systematically to ensure the protection of patient data, compliance with regulatory requirements, and the continuity of pathology services. The risk identification process focuses on both internal and external threats.

Risk Assessment: Each identified risk is rated based on its likelihood of occurrence and potential impact on confidentiality, integrity, and availability of data. High-priority risks are addressed immediately, while lower-priority risks are monitored and managed as necessary.

Mitigation Strategies: Mitigation strategies are developed to minimize risks to an acceptable level. Synnovis continually evaluates the effectiveness of its mitigation strategies and updates them as needed, based on emerging threats, advancements in technology, and changes in regulatory requirements.

2.2. Risk Evaluation Criteria

Asset Value: Asset value at Synnovis is determined based on the criticality of information and systems required to deliver pathology and diagnostic services, protect patient privacy, and maintain operational continuity.

Vulnerability Severity: Vulnerability severity is assessed by determining the potential exploitability of weaknesses in Synnovis's systems, networks, and processes.

Threat Likelihood: Threat likelihood is evaluated based on the probability that specific threats, such as cyber attacks, data breaches, or natural disasters, will exploit identified vulnerabilities.

Risk Threshold: Risk threshold represents the maximum level of acceptable risk for Synnovis. Establishing a risk threshold helps Synnovis decide when to escalate risk mitigation measures and ensures alignment with regulatory and organizational standards, particularly for risks that could affect patient privacy or service continuity.

2.3. Impact Criteria

Confidentiality: A confidentiality breach could lead to unauthorized disclosure of patient data, resulting in legal consequences, loss of patient trust, and potential financial penalties.

Integrity: Compromising data integrity could lead to erroneous diagnostic results, impacting patient care and possibly causing harm.

Availability: A disruption in system availability could delay test results, negatively impacting patient care and eroding trust in Synnovis's services.

Reputation: A security incident or data breach could harm Synnovis's reputation, leading to a loss of clients, challenges in partnerships, and decreased public trust.

Public Safety: Any compromise in Synnovis's diagnostic capabilities, particularly in emergency health situations, could have a direct impact on public safety, delaying diagnoses and potentially exacerbating health risks.

2.3. Risk Acceptance Criteria

Synnovis's risk acceptance criteria are guided by stringent legal and regulatory requirements, including GDPR and NHS Information Governance policies.

Legal and Regulatory Compliance: Synnovis only accepts risks that do not compromise compliance with data protection laws and healthcare regulations. Any risk that could result in non-compliance and potential penalties or legal liabilities is deemed unacceptable.

Impact on Public Safety: Risks that could jeopardize the accuracy or availability of diagnostic services have a lower acceptance threshold.

Risks that interfere with Synnovis's ability to provide timely and accurate diagnostic results, particularly in urgent cases, are treated with priority.

Confidentiality of Sensitive Information: Any risk that could lead to unauthorized access, loss, or exposure of sensitive data might have a lower acceptance threshold.

Acceptable risks are those that can be mitigated to ensure strong confidentiality controls are in place, including encryption, access restrictions, and regular audits.

Integrity of Diagnostic Results: Risks that could compromise the accuracy or integrity of diagnostic results might need to be accepted at a lower level, as they may impact clinical decisions and patient health outcomes.

3. Scope and Boundaries

The **Synnovis Information Security Policy** covers all systems, data, and personnel involved in providing pathology and diagnostic services, focusing on safeguarding sensitive patient information and maintaining secure operations.

- **Covered Systems**: Includes Laboratory Information Management Systems (LIMS), Electronic Health Record (EHR) integrations, diagnostic equipment, and data storage solutions.
- **Data Types**: Protects patient health information, operational data, and diagnostic records, all of which are subject to regulatory standards like GDPR.
- **Internal and External Boundaries:**
    - **Internal**: Applies to all Synnovis facilities, including central and local labs, ensuring secure handling and access control across departments.
    - **External**: Extends to third-party vendors, SYNLAB, and NHS partners, with whom Synnovis shares data under strict data-sharing agreements and compliance guidelines.

4. Organization and Responsibilities

Synnovis oversees providing pathology and diagnostic services, ensuring secure handling of sensitive patient data and maintaining operational integrity. It has designated roles to support data security, regulatory compliance, and effective risk management.

- **Information Security**: Led by the Chief Information Security Officer (CISO), the team develops and enforces security policies to protect Synnovis's information systems and patient data.
- **Data Protection**: The Data Protection Officer (DPO) ensures compliance with data privacy laws, such as GDPR and HIPAA, overseeing data privacy practices across the organization.
- **IT and Cybersecurity**: The IT Security Team manages technical security measures, conducts regular vulnerability assessments, and responds to potential security threats.
- **Clinical Operations**: Clinical staff and laboratory personnel handle patient data in accordance with security protocols, ensuring confidentiality during diagnostic procedures.
- **General Staff and Contractors**: All personnel, including contractors, follow Synnovis's security policies, participate in training, and report any security incidents to maintain a secure working environment.

Synnovis

Document title: Protection of Records Policy

Version: 1.0

Effective date: 22November 2024

3.Protection of Records Policy for Synnovis

3.1 Purpose

The purpose of this policy is to define standards and procedures for accessing Synnovis's information systems and managing documents to protect sensitive patient and operational data. This policy ensures compliance with ISO/IEC 27002 standards and regulatory requirements such as GDPR and HIPAA.

3.2 Scope

This policy applies to all Synnovis employees, contractors, third-party service providers, and any other entities with access to Synnovis's information systems or documents.

3.3 Access Control

- Employees will only be granted access to systems and services that are explicitly authorized for their use.
- Remote access is strictly limited to the official VPN services provided by Synnovis.
- Personal devices are prohibited for tasks associated with public safety and Synnovis operations.
- Physical access to restricted areas is monitored and controlled through security alarms.

3.3.1 Access Request Process

- User access requests must be reviewed and approved via the designated access management process.
- Access rights are granted by relevant departmental supervisors or managers based on operational requirements.
- New employees will receive login credentials linked to biometric authentication, with access permissions assigned by the operations manager.

3.3.2 Principles of Least Privilege

- Access rights will adhere to the principle of least privilege, ensuring employees have only the minimum access necessary for their tasks.
- Access rights will be reviewed and adjusted when an employee changes roles or departments.
- Access will only be approved for specific functions upon request via the access management process and authorized by IT inspectors or commissioners.

3.3.3 Authentication and Authorization

- A robust authentication mechanism will secure user login processes.
- Authorization protocols will define user permissions and access levels.
- Passwords will require mandatory updates every six weeks to enhance security.

3.3.4 Operating System Access Control

- Operating system access is strictly limited to identified and verified users.
- Security measures enforce the use of secure passwords and restrict administrative utilities to authorized IT personnel.
- Privileges are minimized to ensure only essential access is provided to users.

3.3.5 Application and Information Access Control

- Application and data access is restricted to authorized users.
- Systems hosting sensitive information are operated in isolated and secure environments.
- Inactive sessions are automatically terminated, and connection times are restricted to enhance security.
- Role assignments within applications follow the principle of least privilege.

3.3.6 Locking User Accounts

- User accounts will lock automatically after five failed login attempts.
- Locked accounts will only be reactivated after a formal request to the Network Operations Centre (NOC), with the system administrator confirming the action.
- SSH sessions will terminate after 15 minutes of inactivity.

3.4 Data Management

3.4.1 Assignment of Privileges

- Data access privileges are allocated based on job roles and responsibilities, following approval from the relevant department.
- Authorization levels for accessing privileged data assets are set higher than those for non-privileged access.

3.4.2 Access to Data

- An access control framework restricts data centre entry to authorized personnel connected via the Synnovis network. (Refer to the Access Control Policy).

3.4.3 Hard Copy and Media Storage Process

- The storage of data in formats outside the designated data centre servers is prohibited.
- The "Clear Desk and Clear Screen Policy" is strictly enforced to protect sensitive information.
- Classified documents must be stored in accordance with their classification levels and in secure, access-controlled environments such as lockable storage units.
- The use of removable media (e.g., USB drives, disks, tapes) is strictly forbidden.
- Data backups, whether digital or physical, are required for disaster recovery.

3.4.4 Data Transportation Process

- Data (physical or digital) may only be transported outside the data centre under supervision and strictly for disposal purposes.
- Public data communications are secured using HTTPS and TLS 1.3 encryption, while data at rest is encrypted to ensure its safety.
- Data transfers are only permitted when encryption protocols are in place.

3.4.5 Data Destruction Policy

- Physical documents must be shredded into irretrievable fragments, while electronic media must undergo low-level formatting and removal of the master boot record.
- All destruction activities are logged to maintain an audit trail.

3.4.6 Classification of Data

Data is categorized into three levels:

1. **Confidential:** Includes information that could severely harm the organization's interests or security if disclosed. Access is granted strictly on a need-to-know basis.
2. **Restricted:** Covers sensitive information requiring controlled sharing within approved groups.
3. **Public:** Involves data with minimal risk of organizational harm, used for promotional or public-facing purposes.

3.4.7 Electronic Storage

- Digital files are secured against unauthorized internal or external access.
- Confidential and restricted data must be encrypted and backed up regularly.
- Public data is stored with management-approved access controls.

3.4.8 Data Leak Prevention (DLP) Policy

- A DLP tool scans content and attachments to identify unauthorized transmission of sensitive information. Blocked items include personal identifiers, password-protected files, and compressed documents.
- Messages containing sensitive information are automatically flagged and prevented from transmission.

3.4.9 Database Security Policy

- Database access is limited by role-based privileges and stringent authentication processes.
- All input fields are validated to prevent vulnerabilities like cross-site scripting (XSS) and SQL injection attacks.
- Secure communications are ensured using transport layer security (TLS).
- Database activities are monitored through auditing features.

3.4.10 Hardware Security

3.4.10.1 Server and Data Centre Security:

- Physical access to server rooms is restricted to authorized personnel and controlled through biometric authentication systems.

3.4.10.2 Workstations and Laptops:

- Equipment is secured using cable locks, and sensitive devices are stored in secure lockers when not in use.
- A clear desk and clear screen policy is enforced to prevent data exposure.

3.4.10.3 Inventory Management

- A detailed inventory of hardware assets, including serial numbers and assigned users, is maintained and regularly updated.

3.4.10.4 Software Updates and Patch Management

- Surveillance camera firmware and software are updated according to a pre-defined schedule, with patches tested in controlled environments before deployment.
- Regular vulnerability assessments are conducted to address security risks.

3.4.10.5 Training of Staff

- Employees are trained to handle sensitive information and mitigate cybersecurity risks such as phishing and ransomware.
- Staff receive education on appropriate use of work software, devices, and social media to minimize information leaks.
- Information security training sessions are conducted regularly to maintain compliance and reduce the likelihood of errors.

3.4.10.6 Firewall Policy

- All systems must have up-to-date firewalls to safeguard against unauthorized access and cyberattacks, including malware and virus spread.
- Applications and system software must be regularly patched and updated to eliminate vulnerabilities.
- Audit logs of firewall activities will be maintained to monitor and detect any suspicious behaviour.

3.4.10.7 Communication Policy

- During working hours, all staff and officers must use only authorized devices provided by Synnovis for communication. Personal devices are not permitted for official communication.
- Any unauthorized device usage for communication purposes is strictly prohibited.

3.4.10.8 Security of Network

- The Synnovis network will be fully secured to protect all traffic between applications and systems.
- Devices can only connect to the network after undergoing proper authentication processes.
- Comprehensive auditing of network logs will be conducted to detect and respond to suspicious activities.
- Advanced security measures will be implemented to prevent cyberattacks that could compromise the organization’s patients record system.

3.4.10.9 VPN Usage

- Only official VPN services approved by Synnovis may be used to connect to the Synnovis network.
- VPN access permissions are granted based on the nature of the user’s role and the tasks they perform.

Evaluation and Approach regarding using an AI tool (ChatGPT in my case)

In the last part of this assignment, I decided to use ChatGPT more like a guidance tool rather than writing the entire Protection of Records Policy using it.

As you can see in Appenidx 1 Table A , ChatGPT provided a decent structure that I can follow and some ideas about the policies I can implement but they are shallow and very broad. The way it provides some input about the policies is in a broad way and not specific as it would be expected from a areal policy plan and some of the information feels repetitive.

I know AI tools are not able to understand, and they just arrange words in a way that makes sense to us and that makes me think that my abilities and skills are more useful in writing a policy plan.

I agree with it's output as a guidance tool on how to structure and to get some inspiration about what key policies could be implemented and what it's the core meaning of the policy , but I prefer to use my notes from the lectures and laboratories in actually writing the policies instead of slowly feeding the information to ChatGPT hoping it will provide and output I'm satisfied with.

REFRENCES

(International Standards ISO/IEC 27002, 2022)

(GDPR (General Data Protection Regulation), 2023)

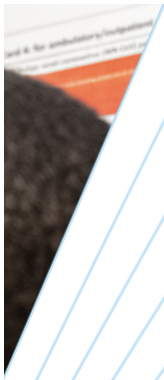
(CVE, 2023)

(UK General Data Protection Regulation (UK GDPR), 2023)

Appendix 1:

Fig A: Images from Synnovis Booklet

The booklet can be found at :https://www.synnovis.co.uk/sites/default/files/upload/SYNNOVIS%20Booklet%20A5%2012pp%20v7%20duo%20quote%20FINAL.pdf



Introduction

On 1 April 2021, SYNLAB formed a 15-plus year pathology partnership with Guy's and St Thomas', and King's College Hospital NHS Foundation Trusts to deliver and transform NHS pathology services across south east London. Its rebranding as Synnovis in October 2022 marked the start of a new relationship between the NHS, SYNLAB and pathology services in the region.

Today, Synnovis serves a population of almost two million people, providing diagnostics, testing and digital pathology services for hospitals, GPs and other NHS healthcare providers, as well as for a number of other private consumers across the UK.

As well as delivering pathology services, Synnovis is responsible for transforming the Trusts' existing hospital-based services into a world-leading, integrated 'hub and spoke' pathology network by 2025. The transformation programme is believed to be one of, if not the, largest in UK healthcare history. It responds to the ambitions set out in the NHS Long-Term Plan, which will not only help to improve the quality of patient care but will also see the NHS save millions of pounds on pathology testing services across the UK.

SYNLAB's NHS partnerships

The Christie Pathology Partnership in Manchester	Pathology First in Essex	Southwest Pathology Services in Somerset	Synnovis in south east London

The Synnovis timeline

Dec 2020

- **SYNLAB and the NHS** agree the future vision for pathology services and confirm shared goals and ambitions, including the delivery of a world-leading, integrated 'hub and spoke' pathology network by 2025.

2021

- The new NHS/SYNLAB partnership commences with SYNLAB taking responsibility for service delivery and transformation (initially retaining the Viapath brand).
- A number of Trust colleagues transfer to the new pathology partnership.
- Colleagues and service user representatives have the opportunity to get involved in developing and agreeing a new name, brand and values for the service.
- Key stakeholders and colleagues are engaged in the development of plans to deliver the overall vision for the partnership.
- Pathology staff associated with GP direct access testing in Bexley, Greenwich and Lewisham transfer over to the partnership.

2022 – 2023

- **New partnership name and brand – Synnovis – launched**
- Online phlebotomy booking system introduced in Southwark and Lambeth.
- Analytical instruments upgraded and harmonised across laboratories.
- Epic Beaker LIMS implemented across six hospitals and six GP boroughs, which consolidates multiple legacy systems and integrates with the Trusts' new Epic electronic health record system.

2024-2025

- Phased introduction of Indexor sample tracking, transport and storage system.
- Phased migration of services into the hub and refurbishment of on-site hospital laboratories.

2025 – Mar 2036

- Service is now 'business as usual', with continuous improvement a part of everyday working practices.
- Around 70% of all pathology activity currently conducted by Synnovis (including all primary care work) processed by the hub.

A tried and tested formula

Pathology partnerships with SYNLAB benefit from access to a global laboratory and diagnostic network and a wide range of clinical, scientific and operational expertise, as well as innovative research and development on an international scale. SYNLAB partnerships also deliver value for money by unlocking increased buying power and economies of scale.

Synnovis: A clinically led approach

The SYNLAB/NHS partnership model ensures that pathology services are led by clinicians. In south east London, Synnovis is responsible for day-to-day service delivery, as well as the transformation programme. The NHS continues to take the lead role in setting the strategic direction of pathology services, linked to the development of other local health and care services.

Headed up by its Medical Director, Synnovis' team of strategic clinical leads works closely with clinical colleagues across the Trusts and is responsible for quality, clinical governance and leadership. This structure ensures that key decisions affecting patient care rest with clinicians, so that clinical excellence is at the heart of all the partnership does.

A hub and spoke pathology model

The hub and spoke model is based on the principle of separating urgent from non-urgent pathology workflows. In its other UK hub and spoke partnerships, SYNLAB has demonstrated that this approach can dramatically improve testing turnaround times and free up valuable estate to use for other patient services.

For Synnovis, a purpose-built, state-of-the-art 'hub' laboratory at Friars Bridge Court in Blackfriars Road is nearing completion, bringing cutting-edge instrumentation, technology and innovation under one roof. On-site hospital laboratories (the 'spokes') will be developed to provide essential services, which focus on the rapid turnaround of urgent tests (e.g. for inpatients or patients attending accident and emergency departments). Some specialist pathology services will continue to be provided at on-site laboratories, in close collaboration with clinical teams.

Synnovis, now one of the largest consolidated pathology networks in the UK, includes the following NHS organisations:

PARTNERS: Guy's and St Thomas' NHS Foundation Trust (includes Royal Brompton and Harefield Hospitals); and King's College Hospital NHS Foundation Trust (includes Princess Royal University Hospital, PRUH)

- South London and Maudsley NHS Foundation Trust
- Oxleas NHS Foundation Trust
- NHS South East London Integrated Care Board, encompassing GP practices, clinics and other community services across the boroughs of Bexley, Bromley, Greenwich, Lewisham, Lambeth and Southwark
- Various NHS tertiary services across the UK

Table A: Table provided in Unit 6

Iteration #	Prompt to ChatGPT	Output	Missing information/Changes/Review
1	can you go through this document and read the first 4 chapters?	The document provided is extensive and detailed, spanning several chapters. It primarily focuses on information security, risk management, and compliance for an organization named Synnovis, with specific reference to standards like GDPR and ISO/IEC 27001. If you'd like, I can extract specific sections or summarize the content for the first four chapters. Let me know how you'd like to proceed!	I've provided my document containing the Context Establishment part hoping to create a bit of context before I start asking for advice writing the policy plan.
2	Assume that you have been appointed as the new CISO, and after a careful study of the existing policies, your team has identified the need of a new Protection of Records Policy to protect Synnovis records from	**1. Purpose** 1. The purpose of this policy is to establish a framework for protecting Synnovis's records from loss, destruction, falsification, unauthorized access, and release. This policy ensures compliance with legal, statutory, regulatory, and contractual requirements while meeting community and societal expectations for the protection and availability of records.	I agree with the structure it provided but it's quite chaotic in my opinion and it's explanations are very shallow. In regards to the policies it provided , they are too broad and omitted specific policies in regards to the network , firewall , vpn , hardware parts and staff training.

	loss, destruction, falsification, unauthorised access and unauthorised release ensuring compliance with legal, statutory, regulatory and contractual requirements, as well as community and societal expectations related to the protection and availability of records.	**2. Scope** 2. This policy applies to all records created, received, maintained, and managed by Synnovis, including physical and electronic formats. It includes all departments, employees, contractors, and third-party vendors handling Synnovis records. **3. Policy Statement** 3. Synnovis is committed to protecting its records to maintain data integrity, confidentiality, and availability, ensuring operational continuity, and fostering trust among stakeholders. **4. Key Objectives** 4. **Preserve Records Integrity** Safeguard records against falsification, unauthorized changes, or loss. 5. **Ensure Accessibility** Maintain records' accessibility for authorized users as required by operational needs and compliance standards.	

		6. **Mitigate Unauthorized Access** Implement controls to prevent unauthorized access, use, or release of records. 7. **Adhere to Legal and Regulatory Requirements** Ensure full compliance with GDPR, ISO/IEC 27001, NHS Information Governance, and other applicable standards. **5. Roles and Responsibilities** 1. **Chief Information Security Officer (CISO)** Oversee policy implementation, regular reviews, and compliance monitoring. 2. **Data Protection Officer (DPO)** Ensure records management aligns with GDPR and data protection requirements. 3. **IT Security Team** Implement and maintain technical security measures for electronic records. 4. **Department Heads** Ensure staff comply	

		with the policy and report any violations. 5. **All Employees** Handle records responsibly and report security incidents. **6. Policy Guidelines** **6.1 Records Creation and Classification** • Classify records as Confidential, Restricted, or Public. • Maintain accurate metadata for all records to track ownership, retention periods, and access rights. **6.2 Records Storage and Preservation** • **Electronic Records:** Store electronic records in encrypted, access-controlled repositories with regular backups. • **Physical Records:** Secure physical records in locked storage with limited access. **6.3 Access Control** • Limit access to records based on the Principle of Least Privilege. • Implement robust authentication mechanisms (e.g.,	

		MFA) for electronic records access. • Maintain logs of all access and changes to sensitive records. **6.4 Protection Against Loss or Destruction** • **Backup Protocols:** Ensure regular backups with offsite storage for disaster recovery. • **Disaster Recovery Plans:** Establish protocols to recover lost or damaged records. **6.5 Protection Against Unauthorized Access** • Implement and regularly update intrusion detection and prevention systems. • Conduct periodic vulnerability assessments and penetration tests. **6.6 Records Retention and Disposal** • Retain records for durations mandated by regulatory or contractual requirements. • Dispose of records securely using shredding, low-level formatting, or degaussing methods.	

		• Maintain disposal logs for audit purposes. **7. Compliance and Monitoring** • Conduct annual audits to ensure policy adherence and identify gaps. • Regularly review the policy to address changes in legal, regulatory, or operational requirements. • Report incidents of non-compliance to the CISO and take corrective action. **8. Enforcement** 8. Any violations of this policy will be subject to disciplinary action in accordance with Synnovis's Employee Code of Conduct and applicable legal requirements.	
3	please kindly highlight 7-15 key elements to include in the Access Control policy	**Key Elements for an Access Control Policy** **1. Purpose and Scope** ○ **Define the objective of the policy: controlling access to**	This output is more useful as it is a good starting point for most of the policies. The output needs to be changed so it can be specifically applied to Synnovis landscape , but I agree with most of it.

		information systems, applications, and records to ensure data integrity, confidentiality, and availability. ○ **Specify who the policy applies to, including employees, contractors, and third-party vendors.** **2. Access Authorization** ○ **Outline the process for granting, modifying, and revoking access based on job roles and responsibilities.** ○ **Ensure that access requests are documented, approved, and periodically reviewed.** **3. Principle of Least Privilege** ○ **Ensure that users are granted the minimum**	

		level of access necessary to perform their job functions. **4. Multi-Factor Authentication (MFA)** **o Enforce MFA for all remote and high-privilege access points to enhance security.** **5. User Account Management** **o Require unique credentials for each user and prohibit shared accounts.** **o Define processes for account creation, modification, and deletion (e.g., deactivation upon termination or role change).** **6. Role-Based Access Control (RBAC)** **o Implement RBAC to align access permissions with job roles, minimizing the risk of**	

		over-provisioning. **7. Access Monitoring and Logging** **o Maintain logs of access activities, including successful and failed login attempts, to support audit and incident investigation.** **8. Session Management** **o Define session timeout periods (e.g., 15 minutes of inactivity) and automatic logout procedures.** **9. Remote Access Policies** **o Permit remote access only via secure VPN connections with encryption.** **o Prohibit the use of personal devices for accessing sensitive information unless explicitly**	

		authorized and secured. **10. Physical Access Control** **○ Limit access to secure areas (e.g., server rooms) using biometric authentication, keycards, or other physical security measures.** **11. Access Reviews and Audits** **○ Conduct quarterly or semi-annual reviews of access permissions to ensure alignment with current job roles and compliance requirements.** **12. Access Termination** **○ Immediately revoke access upon employment termination, role transfer, or other changes affecting access requirements.**	

		13. Third-Party and Vendor Access ○ **Establish strict guidelines for granting access to third-party vendors, ensuring compliance with data protection agreements.** ○ **Limit vendor access to specific systems and timeframes.** **14. Password Management** ○ **Require complex passwords and enforce regular password changes (e.g., every 90 days).** ○ **Prohibit the reuse of previous passwords.** **15. Incident Reporting and Management** ○ **Define procedures for reporting and responding to unauthorized access**	

		attempts or breaches. ○ **Include escalation processes and contact points for security teams.**	
4	please kindly highlight 7-15 key elements to include in the Data Managemen t policy	**1. Purpose and Scope** ○ **Define the purpose of the policy: ensuring the proper handling, storage, and security of data across its lifecycle.** ○ **Specify the scope, covering all types of data (e.g., patient health data, operational data, financial data) and applicable stakeholders (employees, contractors, third-party vendors).** **2. Data Classification** ○ **Categorize data into tiers (e.g., Confidential, Restricted, Public) based**	This provided some policies that were missing from the 2nd iteration, but still not touching the hardware part or the network. In my opinion, some of the information provided can be used to write sub policies instead of putting it under one large policy.

		on sensitivity and impact. ○ **Specify handling and security requirements for each classification level.** **3. Data Ownership and Accountability** ○ **Assign data ownership roles, such as Data Owners (responsible for governance) and Data Custodians (responsible for operational tasks).** ○ **Define accountability for data integrity, confidentiality, and availability.** **4. Data Security and Encryption** ○ **Enforce encryption standards (e.g., TLS 1.3, AES-256) for data at rest and in transit.** ○ **Implement data masking for sensitive information in**	

		non-production environments. **5. Data Retention and Archiving** **○ Define retention periods for different data types in compliance with legal, regulatory, and operational requirements.** **○ Specify processes for securely archiving data that is no longer actively used but must be retained.** **6. Data Access Control** **○ Limit access to data based on the Principle of Least Privilege.** **○ Implement role-based access controls (RBAC) and maintain detailed access logs.** **7. Data Backup and Recovery**	

		○ **Define backup schedules, storage locations, and retention periods.** ○ **Establish a disaster recovery plan to restore data in the event of loss or corruption.** **8. Data Integrity Measures** ○ **Implement checks to ensure data accuracy and prevent unauthorized modification.** ○ **Use hashing algorithms or digital signatures for data verification.** **9. Data Sharing and Transmission** ○ **Define protocols for sharing data internally and externally, including secure transmission methods (e.g., HTTPS, SFTP).** ○ **Ensure third-party**	

		agreements specify data protection responsibilities. **10. Data Disposal and Destruction** **○ Specify secure methods for disposing of data, such as shredding physical documents or low-level formatting of electronic media.** **○ Maintain logs of all data destruction activities for audit purposes.** **11. Compliance with Legal and Regulatory Requirements** **○ Align data management practices with GDPR, HIPAA, and other applicable regulations.** **○ Conduct regular audits to verify compliance.** **12. Incident Management**	

		○ **Define procedures for responding to data breaches, including reporting timelines and mitigation measures.** ○ **Include roles and responsibilities for incident response teams.** **13. Training and Awareness** ○ **Provide mandatory training for employees on data handling best practices, privacy, and regulatory compliance.** ○ **Include awareness campaigns on phishing and social engineering threats.** **14. Data Leak Prevention (DLP)** ○ **Deploy DLP tools to monitor and block unauthorized transmission**	

		of sensitive data via email or file-sharing platforms. ○ **Implement alerts for suspicious activities.** **15. Monitoring and Auditing** ○ **Conduct regular reviews and audits of data handling practices to identify risks and areas for improvement.** ○ **Use monitoring tools to detect unauthorized access or suspicious activities.**	
5	in the case of Synnevo's protection of records policy , what other key policies do you think are crucial and were omitted until now?	**1. Data Privacy Policy** • **Focuses on ensuring compliance with data protection regulations like GDPR, HIPAA, and NHS Information Governance.** • **Specifies how personal and sensitive data is collected,**	This time it just repeated what was in the previous iterations, but it just changed the order and some of the policies information can be written as a sub category of a policy.

		processed, stored, and shared. • **Includes details on data subject rights, such as access, correction, and erasure.** **2. Incident Response and Breach Notification Policy** • **Outlines procedures for identifying, reporting, and managing security incidents and data breaches.** • **Specifies timelines and protocols for notifying regulatory authorities, affected individuals, and stakeholders.** • **Includes roles and responsibilities of the incident response team.** **3. Third-Party Vendor Management Policy** • **Governs how third-party vendors are assessed, onboarded, and monitored for compliance with Synnevo's standards.** • **Includes clauses for data protection, confidentiality, and termination**	

		procedures in contracts. • **Establishes auditing processes for vendor security practices.** **4. Remote Access and BYOD (Bring Your Own Device) Policy** • **Sets rules for remote access to Synnevo's systems and records.** • **Prohibits or secures the use of personal devices for accessing sensitive data.** • **Enforces multi-factor authentication (MFA) and secure VPN usage.** **5. Records Retention and Disposal Policy** • **Defines retention periods for various categories of records to ensure compliance with legal and regulatory requirements.** • **Outlines secure methods for record disposal, such as shredding, degaussing, or incineration.** • **Includes procedures for maintaining logs**	

		of destruction for audit purposes. **6. Physical Security Policy** • **Covers the protection of physical records and infrastructure housing electronic systems (e.g., data centers, labs, and offices).** • **Specifies controls like locked storage, surveillance systems, access badges, and biometric authentication.** **7. Information Classification and Labeling Policy** • **Establishes categories for information sensitivity (e.g., Public, Restricted, Confidential) and corresponding handling requirements.** • **Ensures records are labeled appropriately based on their classification.** • **Aligns with data handling and access control policies.**	

		8. Backup and Disaster Recovery Policy • **Details the frequency, storage locations, and testing of backup systems.** • **Specifies recovery time objectives (RTO) and recovery point objectives (RPO) for critical records.** • **Includes offsite and cloud-based backup requirements.** **9. Audit and Compliance Monitoring Policy** • **Specifies regular audits to verify adherence to all information security and record protection policies.** • **Establishes procedures for reviewing system logs, access records, and compliance with standards like GDPR and ISO/IEC 27001.** • **Includes reporting mechanisms for findings and corrective actions.** **10. Employee Awareness and Training Policy**	

		• **Mandates training for all employees on records protection, data handling, and regulatory compliance.** • **Includes periodic refresher courses and phishing simulation exercises.** • **Tracks and certifies completion of training programs.** **11. Data Sharing and Collaboration Policy** • **Outlines protocols for sharing records within the organization and with external entities.** • **Ensures secure transmission methods (e.g., HTTPS, SFTP) and encryption for sensitive data.** • **Includes clauses for data-sharing agreements with partners.** **12. Encryption Policy** • **Establishes encryption standards for protecting records during storage and transmission.**	

		• **Specifies the use of strong algorithms like AES-256 for encryption.** • **Covers key management practices, including rotation and secure storage.** **13. Vulnerability Management and Patch Policy** • **Focuses on identifying and mitigating vulnerabilities in systems storing or processing records.** • **Mandates timely updates and patch management for software and hardware.** • **Includes regular vulnerability assessments and penetration testing.** **14. Business Continuity Policy** • **Ensures operational resilience by addressing potential disruptions to records availability.** • **Specifies continuity plans for accessing and managing records during emergencies.**	

		15. User Access Review and Revocation Policy • **Ensures periodic reviews of access permissions to align with job roles.** • **Mandates immediate revocation of access for terminated or transferred employees.** • **Aligns with role-based access controls (RBAC) to prevent unauthorized access.**	