Security and Risk Management Portal Risk Assessment Report

Security Analyst Echomedic Project Team

1. EXECUTIVE SUMMARY

1.1. Assessment Overview

A thorough information security risk assessment for Echomedic's suggested security and risk management portal is presented in this document. The assessment was carried out in compliance with the GDPR (General Data Protection Regulation) and Normen (Norwegian health sector regulations) and ISO/IEC 27005:2022 risk management approach.

Every facet of the proposed portal is covered by the risk assessment, including:
Web-based user interface (Angular/React frontend) - Mechanisms for user permission and authentication

- The risk register module is used to record and monitor security threats.
- A library of security policies and processes
- Backend REST API (Express/Node.js)
- PostgreSQL database infrastructure
- The ability to log and monitor

1.2 Key Findings

TOTAL RISKS IDENTIFIED: 15

Risk Level Distribution:

CRITICAL (RED)	**4**	**27%**
HIGH (YELLOW)	**10**	**67%**
LOW (GREEN)	**1**	**6%**

Risk Category Breakdown:

There are nine (60%) technical risks.
Organizational Hazards: Four (27%)
Process Hazards: 2 (13%)
Legal and Privacy Risks: 1 (included in Organizational)

Current Security Posture:

Compliance with ISO 27001: approximately 35% (significant gaps found)
Normen Compliance: around 40% (missing critical controls)
GDPR Compliance: around 45% (insufficient privacy controls)

1.3. Critical Risks Summary

Prior to system implementation, the following four CRITICAL risks need to be addressed:

RISK R001: Weak Password Security (Score: 9/9)

Issue: Weak passwords, such as "123456," can be created by users, leaving accounts open to brute force attacks.

Impacts include: - Unauthorized access to patient data; - Violation of GDPR Article 32, which might result in a €20 million fine; - Loss of patient trust and reputational harm

Enforce passwords with at least 12 characters and complexity criteria as a solution.
After five unsuccessful tries, the account is locked.
The expiration policy and password strength meter

Estimated Implementation: 16 hours

RISK R003: Unencrypted Data Storage (Score: 9/9)

The issue is that private patient information is kept in a database in plaintext without encryption.

Impact: Direct GDPR Article 32 violation
If compromised, a breach must be reported within 72 hours; there might be a fine of €20 million, or 4% of worldwide income; and there could be serious reputational harm.

Solution: TLS 1.3 for data in transit; - AES-256 encryption for all sensitive data at rest; - Secure key management (AWS KMS or Azure Key Vault)

Implementation time estimated: 32 hours

RISK R004: No Multi-Factor Authentication (Score: 9/9)

Problem: There is no second authentication factor for administrator accounts, which are simply password-protected.

Impact: If the admin password is stolen, the entire system is compromised.
Attackers can alter risks, erase logs, and view all data.
Lack of protection against phishing assaults

The solution is to make 2FA mandatory for all admin accounts.
Implementing TOTP (Google Authenticator, Authy) and using backup codes to retrieve accounts

Estimated Implementation: 20 hours

RISK R009: Insecure API Endpoints (Score: 9/9)

Problem: Direct data tampering is possible using REST APIs that are available without authentication.

Impact: All frontend security restrictions are circumvented; - Anyone who knows URLs can access or alter data; - There is no audit trace of who accessed what.

JWT token authentication on ALL API endpoints is the solution.
Limiting the rate to 100 requests per minute and enforcing HTTPS

Estimated Implementation: 24 hours.

1.4 Risk Reduction Strategy

Following the implementation of every suggested mitigation strategy:

	Before	After
CRITICAL Risks (RED)	4	0
HIGH Risks (YELLOW)	10	3
LOW Risks (GREEN)	1	12
Total Risk Score	96	38
Risk Reduction	-	60%
ISO 27001 Compliance	35%	85%
Normen Compliance	35%	90%
GDPR Compliance	45%	95%

2. INTRODUCTION

2.1 Purpose

This risk assessment's objective is to:

1. Determine the information security risks that Echomedic's security and risk management portal faces, such as risks to the confidentiality of patient data, system availability, regulatory compliance, and organizational reputation.

2. Using a methodical assessment of threat sources, vulnerabilities, and attack scenarios, analyze the probability and possible impact of each discovered risk.

3. Determine treatment priorities based on severity, compliance requirements, and business effect by evaluating risks against predetermined criteria.

4. PROPOSE suitable and economical mitigation strategies in accordance with industry best practices, GDPR data protection principles, Normen health sector standards, and ISO/IEC 27001:2022 security procedures.

5. To help Echomedic achieve its objective of creating a sophisticated information security management system, provide a basis for well-informed security decision-making and resource allocation.

Echomedic's strategic goals of establishing a methodical framework for continuous risk management and exhibiting maturity in information security management are supported by this assessment. Building confidence with patients, partners, and stakeholders; ensuring GDPR compliance for patient data processing; and becoming ready for future ISO 27001 certification

2.2 Scope

IN SCOPE:

The following elements of the Echomedic security portal are covered by this risk assessment:

Layer of Application:

Front-end web application using the Angular or React framework
Backend REST API (Express framework with Node.js)
Functionality of the risk register (create, read, update, delete actions)
The document management system and policy library

The interface for user management and administration
Features for dashboards and reporting

Layer of Infrastructure:

Data storage and a PostgreSQL database server
Network architecture and connectivity; Web server and application hosting environment
Cloud infrastructure (on-premises, AWS, or Azure)

Security Domains:

- Mechanisms for authentication (password management, session handling, login)
- Access control and authorization (role-based permissions)
- Data protection (secure storage, encryption in transit and at rest)
- Application security (secure coding techniques, input validation)
- API security (HTTPS, rate limitation, and authentication)
- Monitoring and recording (security events, audit trails)
- Disaster recovery and backup
- Response to incidents and business continuity

Data Resources:

- Health information and patient IDs (if processed by the system)
- Personal information (emails, names, roles) and user credentials
- Data from risk assessments and security records
- Policies and procedures related to security
- Audit trails and system logs
- Source code and configuration files for applications
- Cryptographic certificates and keys

Compliance Conditions:

- ISO/IEC 27001:2022:
- Information Security Management System; Normen.
- Norwegian Health Sector Information Security Standard; GDPR.
- General Data Protection Regulation (EU) 2016/679.
- Norwegian Personal Data Act: Regulations unique to the healthcare industry

OUT OF SCOPE:

This evaluation does not include the following areas:

- Echomedic's current legacy apps and systems
- Third-party providers' internal activities (only vendor interfaces evaluated)
- Access restrictions and physical office security
- HR practices (employment contracts, background checks)
- Legal and contractual considerations that go beyond technical security measures

- Analysis of financial and business risks with a sole focus on information security
- Activities related to marketing and business growth

2.3 Regulatory Context

Strict information security safeguards are necessary since Echomedic operates in a complicated regulatory environment:

Information Security Management ISO/IEC 27001:2022
The international standard for information security management systems (ISMS) is ISO 27001.

Important prerequisites include:

- A methodical approach to handling confidential firm data; - A risk-based approach to detecting and addressing security threats
- 93 security controls have been implemented in 14 domains (Annex A).
- Frequent evaluation, monitoring, and mechanisms for ongoing improvement
- Thorough policy and procedure documentation
- The dedication of management and sufficient distribution of resources

Relevant Control Categories in Annex A:
A.5 Controls within the organization (37 controls)
A.6 Human controls (eight controls)
A.7 Physical controls (14 controls)
A.8 Technical controls (34 controls)

Benefits for Echomedic include: International recognition and reputation in the healthcare industry; - a competitive edge in contract bidding; - a framework for methodical security management; - a basis for partner and customer trust; and - a demonstration of due diligence to regulators and auditors.

Norwegian Health Sector Standard, or Normen

For Norwegian healthcare organizations, Normen has certain security standards.

Important areas pertinent to this evaluation:

4.1 Security Awareness and Training:
Every employee must undergo yearly refresher training; receive specialized training for managing patient data and health information; and be aware of phishing, social engineering, and insider threats.

4.2 Authentication and Access Control:

All users must use robust authentication methods, and privileged accounts must use multi-factor authentication.

Implementing role-based access control (RBAC) and conducting frequent access reviews and recertification (at least quarterly)

The least privilege principle is upheld; access is immediately revoked upon termination.

4.3 Confidentiality and Encryption:
Strong algorithms (AES-256) are used to encrypt patient data while it is at rest.
Data encryption during transmission with TLS 1.2 minimum
Procedures for secure key management
Preventing improper sharing of private health information

4.4 Availability and Business Continuity:
Regular testing of backup and restoration processes; established procedures for disaster recovery planning
High accessibility for vital healthcare systems
Recovery Time Objective (RTO) established for important systems; DDoS prevention measures for internet-facing systems

4.5 Secure Development Lifecycle:
OWASP-compliant secure coding techniques; integration of security needs into the system design phase Vulnerability management and prompt patching; code review and security testing prior to deployment; and change management protocols include security review.

4.6 Monitoring and Logging:
Thorough audit recording of all patient data access
Monitoring and alerting capabilities for security events
Minimum 12-month log retention (longer for key events)
Log integrity protection (read-only storage)
Frequent examination of logs for questionable activity

4.7 Supplier and Third-Party Management
Vendor security evaluations prior to engagement; data processing contracts with security specifications Frequent audits and assessments of vendor security Contractual provisions granting the right to audit; requirements for reporting incidents.

The General Data Protection Regulation, or GDPR

GDPR places stringent restrictions on how EU citizens' personal data is processed.

Important Articles for This Evaluation:

Article 5: Processing Principles
The legality, equity, and openness of data processing
Limitation of purpose (data used only for specified purposes)
Minimize data by gathering only what is required.
Accuracy (maintain current personal data)
Limitation on storage (don't retain longer than necessary)
Confidentiality and integrity (security principle)
Accountability (show adherence)

Article 25: Data Protection by Default and by Design
Put in place the necessary organizational and technological measures
Privacy should be protected by default settings (opt-in, not opt-out) from the very beginning of the design process.
By default, pseudonymization and minimization.

Article 32: Processing Security
Personal data can be encrypted and pseudonymized; confidentiality, integrity, availability, and resilience can be maintained; availability and access can be restored following incidents.
Frequent testing and assessment of security measures; security measures suitable for the degree of risk

Article 33: Notifying the Supervisory Authority of a Breach
Notify the supervisory authority of any breach within 72 hours of learning about it. Record all breaches involving personal data, even if they are not reported.
Evaluate the risk to people's rights and freedoms; notify them of the breach, its anticipated repercussions, and the corrective actions that need to be taken.

Article 34: Notifying Data Subjects of Breach:
Notify those impacted if there is a high risk to their rights; explain the breach in plain language; and offer suggestions for self-defense.

Article 35: Data Protection Impact Assessment (DPIA):
Required for processing that could pose a serious risk
Processing procedures are systematically described; need and proportionality are evaluated; and dangers to people's rights and freedoms are evaluated.
Actions to deal with and lessen dangers

Article 37: Data Protection Officer (DPO)
It is necessary for public bodies and organizations that process health data; the DPO must be well-versed in data protection law; it is a position of independence that reports directly to upper management.
Access and resources required to carry out tasks

Penalties for Failure to Comply:

Up to €20 million or 4% of the world's yearly turnover, whichever is more
Reputational harm and a decline in patient and customer trust; possible civil litigation from impacted parties Regulatory audits and investigations.

Echomedic must comply with the following GDPR requirements:

- Consent-based management mechanisms for data collection.
- Legal basis for processing personal data (consent, legitimate interest, etc.).
- Right to access (respond to requests from data subjects within 30 days).
- Right to erasure ("right to be forgotten") functionality.
- Right to data portability (export data in machine-readable format).
- Clear privacy notices and transparency regarding data use.
- Appointment of a Data Protection Officer (DPO).
- Records of processing activities (Article 30).
- Agreements with data processors (data processing vendors).
- International data transfer protections (if data exits the EU).

3. RISK ASSESSMENT METHODOLOGY

3.1 Framework and Standards

The approach used for this risk evaluation is based on globally accepted standards:

PRIMARY FRAMEWORK:
The main framework is ISO/IEC 27005:2022. Information Security Risk Management:
Complies with ISO 27001 ISMS criteria; offers instructions for information security risk management procedures.
Endorses a risk-based strategy for putting security controls in place

SUPPORTING STANDARDS:
ISO/IEC 27001:2022 ISO/IEC 27002:2022; Annex A controls and ISMS requirements NIST SP 800-30 Rev. 1. Guide for Conducting Risk Assessments. Information Security Controls Reference Guide
The framework for risk management and the NIST Cybersecurity Framework (CSF).

BEST PRACTICES INDUSTRY:
The Open Web Application Security Project's (OWASP) Top 10 Web Application Security Risks for 2021.
The Application Security Verification Standard (ASVS) of OWASP
The Center for Internet Security's CIS Controls v8
The Top 25 Most Dangerous Software Errors by SANS

3.2 Risk Assessment Process

Based on ISO 27005, the risk assessment employs a methodical four-phase process:

PHASE 1: CONTEXT ESTABLISHMENT

Activities:

- Clearly define the goals and scope of the assessment
- Determine the stakeholders (development team, security team, management, users)
- Create risk assessment standards (impact and likelihood scales)
- Establish thresholds and criteria for risk acceptance

Methods Employed:

- Review of comparable healthcare application risk assessments.
- Stakeholder interviews with project team members.
- Document review (system architecture diagrams, requirements specifications)
- Analysis of regulatory requirements (ISO 27001, Normen, GDPR)

Results:

- Defined scope statement with includes and exclusions
- A matrix of risk evaluation criteria and a stakeholder registration with roles and responsibilities

Phase 2: Identification of Risk

Activities:

1. Determine and categorize information assets and their organizational value.
2. Determine internal and external threat sources.
3. Determine system and process vulnerabilities and weaknesses
4. Determine the efficacy of current security measures
5. Record possible danger situations and ways to attack

Techniques Used:
Eight team members (three frontend engineers and five cybersecurity students) participated in a risk training with a cross-functional team in December 2024.
The assisted session lasted for three hours.

The STRIDE threat modeling approach:

- Identity spoofing and data tampering
- The act of repudiation
- Disclosure of Information and Denial of Service
- Increasing Privilege
- Analysis of attack trees for high-risk situations

- Results of the vulnerability assessment from the initial code review
- The application for the OWASP Top 10 checklist
- Industry publications that provide threat intelligence for the healthcare sector

Results:
Asset inventory classified according to availability, confidentiality, and integrity
A thorough threat catalog and a list of vulnerabilities with severity ratings
15 hazards were recognized in the first risk register.

PHASE 3: RISK ANALYSIS

Activities:

1. Determine the probability that each risk scenario will materialize
2. Evaluate possible effects on business, technology, compliance, and reputation.
3. Determine the degree of risk (probability × impact).
4. Assess the efficiency of current controls

Techniques Used:

- Qualitative risk analysis with a likelihood and impact scale of 1 to 3
- Cybersecurity team members' expert opinion - Historical incident data from comparable healthcare applications.
- Data breach reports and industry statistics (Verizon DBIR, IBM Cost of Data Breach).
- Evaluation of control efficiency in relation to ISO 27001 standards.

Results:

- Likelihood scores accompanied by thorough explanations
- Business impact analysis combined with impact scores
- Risk ratings were computed (1–9 scale).
- Risk categorization (RED, YELLOW, GREEN) - Evaluations of control efficacy.

PHASE 4: RISK EVALUATION AND TREATMENT PLANNING

Activities:
1. Examine computed risk levels in relation to risk acceptability standards
2. Set treatment priorities for hazards according to their seriousness and business effect.
3. Choose the best course of action (avoid, decrease, transfer, accept).
4. Create thorough mitigation strategies with targeted controls
5. Determine the remaining risk following suggested mitigating

Techniques Used:
- To see the distribution of risks, use risk matrix mapping.

- Cost-benefit evaluation of mitigating strategies
- ISO 27001 Annex A control selection; ISO/Normen/GDPR compliance gap analysis
- Calculating residual risk and evaluating acceptability

Results:

- A prioritized risk registry that includes treatment choices
- A thorough risk management strategy with a schedule for execution
- Cost estimates and resource requirements for every mitigation
- Assessment of residual risk demonstrating anticipated risk decrease.

3.3 Risk Evaluation Criteria

LIKELIHOOD ASSESSMENT (1-3 Scale)

Score	Level	Description
1	Unlikely	The event is unlikely to occur in the near future. Less than 10% is the annual probability. Anticipated Frequency: Every ten or more years Examples include insider sabotage (with appropriate controls), nation-state targeted attacks on small organizations, and natural disasters at data centers.
2	Possible	An event could take place in specific situations. Probability per year: 10–50% Anticipated Frequency: Every two to ten years Examples SQL injection if code is improperly evaluated; hardware failure without redundancy; and targeted phishing campaigns.

3	Likely	The event is anticipated to happen frequently. Annual Probability: Over 50% Anticipated Frequency: Several times annually Examples: Automated vulnerability scans; phishing emails directed at employees; and brute force efforts on weak passwords.

The following factors are taken into account when determining the likelihood of an event:

- Historical incident data (internal breaches and industry-wide trends)
- Known vulnerabilities and exposure level
- Threat actor capability, resources, and motivation
- Attack surface size and ease of exploitation
- Effectiveness of current preventive controls
- Environmental factors (internet-facing vs. internal systems)
- Industry targeting (healthcare is a high-value target)

IMPACT ASSESSMENT (1-3 Scale)

Score	**Level**	**Consequences**
1	Low	**Operational**: Less than 10 users were impacted. Service interruption lasted less than 4 hours. There are workarounds available; there is only a slight inconvenience and no permanent data loss. **Financial:** No significant financial impact on the company No need for an insurance claim **REPUTATIONAL:** Small, limited occurrence. Only local/internal impact. No media coverage.

		Minimal impact on trust. **COMPLIANCE:** There is no need for regulatory reporting. There is a small infraction of internal policy.
2	Low	**COMPLIANCE**: Required regulatory reporting. Possible warnings or small penalties **ISO 27001 audit** non-conformity (correctable) More supervision is needed.
3	High	**OPERATIONAL**: More than 100 users were impacted. Service interruption lasting longer than 24 hours. Serious data loss or corruption; A significant data breach involving more than 100 records. A threat to business continuity **REPUTATIONAL**: Serious harm to the company's reputation. Attention from national and international media, Loss of patient and consumer trust, which is hard to regain. Competitive disadvantage. Loss of business opportunities **COMPLIANCE**: Notification of GDPR breaches must be given within 72 hours.

		Potential license suspension or regulatory penalties. legal action from impacted parties; the possibility of ISO 27001 certification being revoked or at danger; and several regulatory investigations. **PATIENT SAFETY:** Possible effects on patient care or safety. compromised health information confidentiality. breach of doctor-patient privilege

RISK SCORING MATRIX

Risk Score = Likelihood × Impact

IMPACT →

3 🟢	6 🟡	9 🔴
2 🟢	4 🟡	6 🟡
1 🟢	2 🟢	3 🟡

3.4 Risk Treatment Approach

Based on organizational risk appetite and cost-benefit analysis, one of four treatment approaches is chosen for each identified risk:

Option 1 for Treatment: Avoid

An explanation:

- Get rid of the risk source completely
- Modify the system's architecture to eliminate the vulnerability
- Put an end to the dangerous conduct
- Select a less risky alternative strategy.

When to Apply:

- Risk cannot be sufficiently reduced and is intolerable.
- The activity's benefits are outweighed by the cost of mitigation.
- There are other methods that have a reduced risk profile.
- Activity is not necessary for key company operations.

For instance:

- Not putting in place a risky feature that isn't necessary
- Deciding not to keep some kinds of sensitive information
- Replacing custom development with a tried-and-true third-party solution

Option 2 for Treatment: REDUCE (MITIGATE)

An explanation:

- Put security measures in place to reduce the possibility or impact
- The most popular method for handling technical hazards
- Use ISO 27001 Annex A security controls.
- Employ several defensive layers (defense in depth)

When to Apply:

- There is more risk than is reasonable, but action is required.
- There are affordable controllers available.

- After mitigation, residual risk will be acceptable.
- necessary for essential company operations

For instance:

- Implementing input validation to reduce SQL injection risk
- Adding encryption to reduce impact of data breach
- Deploying multi-factor authentication to reduce account compromise

Control Types:

PREVENTIVE: Stop incidents before they occur (firewalls, access control)
DETECTIVE: Identify incidents when they occur (logging, monitoring, IDS)
CORRECTIVE: Minimize impact after incident (backups, incident response)

TREATMENT OPTION 3: TRANSFER (SHARE)

An explanation:

- Give a third party the danger.
- Contracts, insurance, and outsourcing
- The financial and operational damage is shared, but risk is not completely removed.
- Transfer of liability to the insurer or vendor

When to Apply:

- The organization's lack of specialized knowledge
- Self-management is too expensive.
- The financial impact must be distributed or safeguarded.
- Service level agreements offer assurances.

For instance:

- Using SLA-guaranteed managed cloud services (AWS, Azure)
- Financial protection against breaches through cyber insurance
- contracting with MSSP (Managed Security Service Provider) to handle security activities
- Liability provisions in contracts with suppliers

Restrictions

- It is impossible to totally transfer reputational risk.
- GDPR maintains the organization's ultimate accountability and calls for continuous vendor monitoring and supervision.

TREATMENT OPTION 4: ACCEPT

An explanation:

- Recognize the risk and do not act right away.
- The risk is within reasonable bounds.
- must be duly recorded and authorized by management.
- requires constant observation

When to Apply:

- The risk level is within risk appetite and is LOW (GREEN).
- Potential damage is outweighed by mitigation costs.
- There are no workable or affordable controls available.
- The danger is expressly accepted by senior management.

For instance:

- Accepting the risk of a low-probability vendor breach for a reliable supplier
- Taking on less risk from historical features that have been terminated
- Accepting residual risk following the implementation of all feasible controls

Conditions:

- Official risk acceptance signed by the relevant level of management
- recording the justification for acceptance
- Frequent evaluation (at least once a year)
- Keeping an eye on shifts in the threat landscape

4. ASSET IDENTIFICATION

Based on their significance to Echomedic's activities and the consequences of their compromise, critical assets have been identified and categorized as follows:

4.1 Information Asset Inventory

A-01		Identifiers, medical data, treatment histories,	CONFIDENTIAL (Highest)	Data Controller

	Patient Data	diagnoses, and personal health information		
A-02	User Credentials	2FA secrets, session data, authentication tokens, hashes of passwords, and usernames	CONFIDENTIAL	Security Team
A-03	Risk Register Data	determined security threats, evaluations, vulnerability information, and mitigation strategies	INTERNAL	Security Manager
A-04	Security Policies	SOPs, security standards, incident response protocols, and access control rules	INTERNAL	Security Manager
A-05	System Logs	Application logs, audit trails, security events, and access logs	INTERNAL	IT Ops
A-06	Application Code	Source code, configuration files, deployment scripts, and API documentation	INTERNAL	Dev Team
A-07		Secrets, signing keys, SSL/TLS certificates, encryption keys,	RESTRICTED (Absolute Highest)	Security Team

	Cryptographic Keys	and API keys		

4.2 System Assets

ID	Asset Name	Description	Criticalitycd
S-02	Web Application (Frontend)	Reports, dashboards, forms, and user-facing interfaces (Angular and React)	HIGH
S-03	API Server (Backend)	Data processing, integrations, core business logic, and REST API (Node.js/Express)	CRITICAL
S-04	Database Server	PostgreSQL database, single source of truth, and permanent data storage	CRITICAL
S-05	Authentication Service	Password verification, token creation, sessions, login, and 2FA	CRITICAL
S-06	Logging Infrastructure	Audit trails, security logs, and SIEM integration (planned)	HIGH
S-07	Backup System	Disaster recovery, offsite storage, automated backups, and restoration capabilities	HIGH

Asset Classification Definitions:
CONFIDENTIAL (Highest Protection Level):

- Encryption is necessary both in transit and at rest, and access is limited to authorized personnel with a business requirement.
- thorough audit recording of every access
- cannot be distributed externally without permission.
- Data Loss Prevention (DLP) measures implemented
- For instance: User credentials and patient data

Internal (Level of Medium Protection):

- All staff with business needs can access it.
- External sharing should only be done with permission.
- It is advised to log access.
- Typical recovery and backup
- Examples include security rules and risk registers.

Restricted (Highest Absolute):

- Very little access (usually 1-2 people)
- Recommended hardware security modules
- When feasible, use dual control and split knowledge.
- Electronic communications must always be encrypted.
- Physical safety precautions
- For instance: Root certificates and master encryption keys