PROJECT INTRODUCTION

This project is aimed at compiling a compliance report for the Dublin General Hospital, whose main task is to provide healthcare to the population, and determining its compliance based on the GDPR requirements with data security/protection and network security.

This proceses will be conducted in certain steps, which would include: Identifying the company's jewel crown (main assets), analysing the company's adherence to the GDPR General Data Protection Regulation based on these major asset, identify the laws and regulations or frameworks necessary for the data handling resources and processes, confirming that the required roles are being handled by the specified personnels, and identifying and recommending the necessary methods that will ensure that these frameworks are implemeted

I'll be using data from St James Hospital since Dublin General Hospital is only fictional

About Dublin General Hospital

Dublin General Hospital (DGH) is a public acute teaching hospital providing healthcare services in Dublin metropolitan area. As a major healthcare institution in Ireland, DGH processes large quantities of sensitive patient information daily, including medical histories, diagnostic records, treatment plans, prescription information, laboratory results, medical imaging, and billing data.

Key findings:

Dublin's General Hospital's **Crown Jewel** – Electronic health and medical data.

Regulatory Context

GDPR – General Data Protection Regulation, was established in 25th May 2018, to regulate companies' compliance to safety within the EU, and it has a requirement for processing personal data and is also related to DGH's handling of personal data.

Scope and Objectives: We will be using the GDPR to analyse the health and medical data for Dublin General Hospital, and give our recommendations from the analysis results. And this analysis will contain

- Identifying the crown jewel (Health data record)
  - Components essential for handling health data

- Network architecture and data flow
    - Data flowing and mapping
- GDPR application for the data handling, resources, and processes.
    - Health data handling
    - Network Infrastructure & transfer of data
    - Breach consequences
- Compliance verification methodologies
- Recommendations for achieving and maintaining GDPR compliance
- Conclusion

MAIN BODY

1. ELECTRONIC HEALTH REPORT DATA

1.1. Electronic Health Data

For Dublin General Hospital, the most essential information (crown Jewel) requiring protection is the Electronic Health Record System and the patient data it contains. These data include:

a. Demographic Data
    - Full name, D.O.B, address, contact details, PPS numbers, Insurance details

b. Clinical / Medical Data
    - Medical history and chronic conditions, current medications, allergies, treatment plans, diagnostic reports (Paubox 2024)

c. Administrative Data
    - Billing data, consent forms, appointment data, consent forms, discharge forms. (Thomson Reuters Practical Law, 2025)

The health data listed above are very delicate and as classified under the GDPR Article 9. This generally summarizes health data as a special category of data. Unauthorized disclosure could reveal intimate details about patients' physical and mental health, sexual life, genetic information, and biometric data.

Also, EHR integrity and availability are extremely important because inaccurate medication records could result in fatal drug prescriptions with effects; while unavailable records during emergency treatment could delay critical interventions, and finally, a corrupted diagnostic result could lead to misdiagnosis.

So, considering all of these, health data is a life and death matter, and should be handled as such. (Intersoft Consulting)

In Ireland, the Data Protection Commission (DPC) serves as the supervisory authority enforcing GDPR compliance. Non-compliance can result in administrative fines up to €20 million or 4% of global annual turnover (whichever is higher), and reputational damage affecting patient trust. (Intersoft Consulting)

1.2. Essential components for handling health data

Data handling is a duty shared between two parties, the ‘Controller’ and ‘Processor’,

- Controller: acts as the primary point of management for storing data, coordinating data workflow, and configuration. (Intersoft Consulting, 2025)
- Processor: acts only on documented instructions from the controller, implements appropriate technical and organizational measures, and assists the controller in fulfilling data subject rights and supervisory requirements. (Intersoft Consulting, 2025)

and their procedures must incorporate privacy by design principles (GDPR, Article 24 - 43), with specific technical measures and handling, including:

Controller

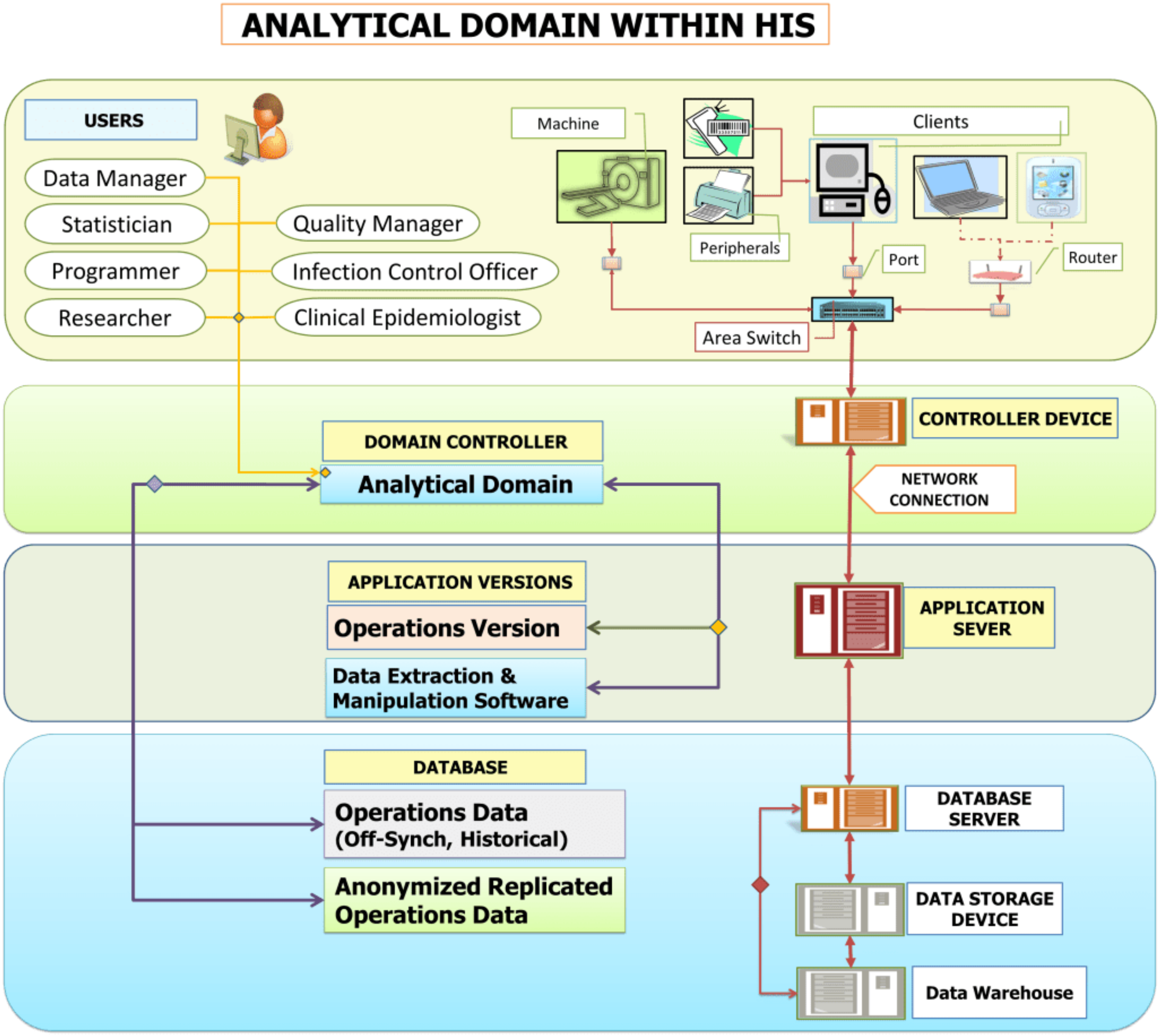
- Quality Data availability & management
- Automated configurations and updates
- Data protection and recovery
- Data monitoring and logging
- Network segmentation and access control

Processor

- Security and access control
- Data encryption
- Data minimization and retention
- Network and endpoint protection

2. NETWORK ARCHITECTURE AND DATA FLOW

2.1. Hospital Network Infrastructure Components



(Drdollah, 2024)

a. Layer 1 (External / Internet zone) Users

- Public-facing website (appointment booking, general information)
- Patient portal for lab results and appointment management
- Gateway for external communications
- VPN gateway for remote staff access
- Firewall / Switch #1 (perimeter defense)

b. Internal network 1 (Data reception level)

- Domain controllers (Active Directory authentication)
- DNS/ Email Servers
- Analytical domain

c. Internal network 2 (Administrative level)
    - Application servers
    - General workstations (non-clinical staff)
    - HR systems
    - Data Extraction and processing

d. Internal network 2 (Administrative level)
    - Primary EHR Database Servers (core patient records)
    - EHR Application Servers (clinical interface)
    - Picture Archiving and Communication System (PACS) - medical imaging storage
    - Laboratory Information System (LIS)
    - Pharmacy Management System & Radiology Information System (RIS)
    - Clinical workstations (doctors, nurses, clinicians)
    - Firewall #2 (internal segmentation between administrative and clinical zones)

Physical Security Zone:

- On-premises data center housing EHR servers
- Backup systems (on-site and off-site encrypted backups)
- Physical access controls (biometric scanners, access badges)
- Environmental controls (temperature, humidity, fire suppression)
- Uninterruptible Power Supply (UPS) and backup generators

External Integrations

- National Health Information System (government health records exchange)
- External Specialist referral hospitals, laboratories (pathology results) & Pharmacies
- Health insurance companies (claims processing)
- General practitioners (GP referrals and discharge summaries)

2.2. Data Flow Mapping / Organizational Structure (National Library of Medicine, No year)

1. Level 1 (Registration / Patient Identification)
    a. Receptionist / Users enter personal data
    b. Data flows through the internal network to the database
    c. System checks for existing patient records / creates a new one
    d. The data record is retrieved

2. Level 2 (Clinical Consultation)
    a. The doctor accesses EHR from a clinical workstation using role-based credentials
    b. The doctor enters clinical notes, diagnoses, and treatment plans.
    c. Sends or orders for diagnostic tests (labs, imaging)
    d. Generated prescriptions are transmitted to the pharmacy system

3. Level 3 (Diagnostic Testing)
    a. Laboratory / Radiology receives diagnostics orders from EHR
    b. Tests and images are captured and stored in the database
    c. Clinician / Radiologist assesses, captures results, and makes decisions
    d. Report and images are sent to the relevant health practitioner, and linked to the patient record in EHR

4. Level 4 (Discharge and External Sharing)
    a. Discharge summary generated from EHR
    b. Summary transmitted securely to the patient's GP via encrypted email or national health information exchange
    c. Patient receives a copy of discharge instructions via the patient portal

5. Level 5 (Backup and Archive)
    a. Patient’s EHR is archived and updated

Healthcare data's sensitivity demands heightened security measures. For this to be achieved, the network and data flow require appropriate technical and organizational measures with top quality, adequate costs, and low risks to rights and freedoms. For health data within the network, this typically requires proper encryption, data monitoring, access controls, and comprehensive audit logging, etc.

3. GDPR APPLICATION

3.1. GDPR Applicable to Health Data Handling

GDPR Articles from 5 – 34 explain in every format how Dublin General Hospital should handle Electronic Health Data. From data collection, data storage, and transfer. I'll highlight some key articles to consider thoroughly:

Article 5: Principles Relating to Processing

- Lawfulness, fairness, transparency (5.1.a): Patients must understand how their data is used
- Purpose limitation (5.1.b): Health data collected for treatment cannot be repurposed for unrelated activities
- Data minimization (5.1.c): Only data necessary for healthcare provision should be collected
- Accuracy (5.1.d): Medical records must be accurate and kept up to date
- Storage limitation (5.1.e): Records retained only as long as legally required
- Integrity and confidentiality (5.1.f): Appropriate security measures required

Article 6: Lawfulness of Processing

Dublin General Hospital must establish a legal basis, primarily by talking about the legal obligation to maintain medical records and the protection of vital interests in emergencies

Article 9: Processing of Special Category of Personal Data

Dublin General Hospital must handle data for healthcare provision and management, subject to professional secrecy obligations (medical confidentiality). It prohibits the hospital from processing data revealing race, politics, religion, trade unions, genetics, biometrics for identification, health data, and sexual life/orientation. Only healthcare-related data, unless specific exceptions apply

Article 25: Data Protection by Design and by Default

Considering that Dublin General Hospital is the main data controller, its EHR systems must embed privacy protections from the initial to final phase, implementing pseudonymisation, encryption, and access controls by default.

Article 32: Security of Processing

This article emphasizes the importance of Dublin General Hospital regarding the security, technical, and organizational measures appropriate to risk, for both the controller and processors, including data encryption, pseudonymization, confidentiality, integrity, availability, resilience, and regular security testing

3.2. GDPR Application to Network Infrastructure and Transfer of Data

GDPR Article 32 explains how Dublin General Hospital should handle Electronic Health Data. I'll highlight some key articles to consider thoroughly:

Article 32 GDPR (Security of processing)

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(a) the pseudonymisation and encryption of personal data;
(b) the ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services;
(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
(d) a process for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. *In assessing the appropriate level of security, account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.*
3. *Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.*
4. *The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.*

Dublin General Hospital network architecture addresses these requirements through:

Article 32(1)(a) - Encryption and Pseudonymization:

- Database encryption to protect data at rest
- TLS encryption to protect data in transit
- Replacing identifiable patient names with pseudonyms)

Article 32(1)(b) - Confidentiality, Integrity, Availability, Resilience:

- Creating Access controls to ensure confidentiality
- Audit logging enables integrity verification
- Providing redundant servers and backup power to ensure availability

Article 32(1)(c) - Restore Availability:

- Daily backup to enable restoration at any time

Article 32(1)(d) - Regular Testing and Assessment:

- DGH must conduct annual penetration testing, vulnerability scanning, and security audits

Article 32(2)

- DGH must always assess risks that are present during processing and apply the appropriate level of security

Article 32(3)

- DGH must adhere to an approved code of conduct and certification for handling data, to be able to demonstrate compliance with the requirements for GDPR

Article 32(4)

- The controller and processor in charge of handling DGH's data must ensure that any person responsible for processing data on behalf of the 'controller/processor' is doing so under direct instruction.

3.3. Data Breach Consequences (Privacy Engine, 2023)

A health data breach in Dublin General Hospital would lead to the following events:

- Exposure of the patient's medical data
- Loss of patient trust in DGH's ability to protect sensitive data.

- Decline/loss of customer loyalty
- Lawsuits from affected individuals seeking compensation
- Investigations by regulatory bodies
- Potential fines and penalties for non-compliance with data protection obligations.
- Incident response, forensics, and system recovery expenses.
- Breaches can lead to a temporary shutdown or even total closure of the organization

4. COMPLIANCE VERIFICATION METHODOLOGIES (Comply Dog, 2025)

This section explains the methods for verifying Dublin General Hospital's compliance with the GDPR for data handling.

4.1. Internal Audit and Assessments

- Comprehensive review of all data processing activities, quarterly or annually.
- Annual or quarterly penetration testing and vulnerability scanning
- Review of third-party processor contracts for GDPR compliance
- Evaluation of training completion rates
- Audit report presented to hospital executive leadership and Board

4.2. External Assessments

- ISO 27001 Certification availability
- Do annual surveillance audits by the certification body verify ongoing compliance

4.3. Technical Monitoring

- Access monitoring: The SIEM system should monitor all EHR access in real-time
- Alerts are triggered for unusual access patterns, like access to VIP records, etc.
- Detection of potential privacy violations, e.g, alert staff accessing records of family/friends without clinical justification

4.4. Documentation Review

- Getting a record of all processing activities, like a comprehensive inventory of all patient data processing activities, and making sure that they're available for DPC inspection
- Version control tracking policy updates
- Reviewing training documentation records and ensuring that the training contents have GDPR compliance covered
- Tracking training completion for all staff

5. RECOMMENDATIONS FOR ACHIEVING AND MAINTAINING GDPR COMPLIANCE (Sprinto, 2025)

Based on the compliance assessment conducted on Dublin General Hospital on their ‘crown jewel - Data’ and its network architecture for the data workflow and handling, I will recommend the following prioritized recommendations, which will enhance DGH's GDPR compliance.

5.1. Appoint a Data Protection Officer

This is key and mandatory to assign roles and responsibilities to someone who can oversee the chain of command. DGH can do this by:

- Recruiting a qualified DPO with healthcare privacy expertise, or get a contract with an external DPO service/company.
- Provide the DPO with necessary resources, data, and executive access to relevant information
- Ensure that the DPO reports to the Chief Executive with the relevant updates

5.2. Establish Data Rights Procedures, Handling, and Breach Procedure

DGH should state and provide formal procedures on how patients' data and rights are handled, including complaints.

- Document procedures for handling data access, rectification, erasure, restriction, and portability requests
- Create standard response templates
- Establish a 24/7 on-call rotation for breach response
- Develop comprehensive breach response plan (e.g., 72-hour notification deadline)

5.3. Compliance Training Program

People are one of the major loopholes to compliance, and training staff on GDPR compliance methods helps reduce human error risks

- There should be specialized training for roles with delicate data access

5.4. Breach Detection and Response Verification

Dublin General Hospital should run regular simulation exercises to ensure breach response capabilities for GDPR compliance

- Exercises simulating various breach scenarios, e.g., Ransomware attack encrypting EHR database

- Measure the time it takes to detect, contain, assess, and notify. (less than 72 hours)

5.5. Documentation Review

Dublin General Hospital should be able to have documentation that can be easily referred to for compliance, which includes:

- A record of all activities
- Ensure that this record is updated on every new activity
- Documentation to confirm training completion tracking for all staff
- Updated training materials are available as per GDPR updates

6. CONCLUSION

Dublin General Hospital's compliance with the General Data Protection Regulation is key to being able to handle its' Crown-Jewel, which is the 'Health Data / Electronic Health Data.' And mismanagement of this data, or any form of breach in this, has very serious consequences, like legal, financial, reputational, and client trust damages.

This report outlines what needs to be done to achieve the main goal of securing and handling this data with GDPR compliance. E.g., appointing data security roles and training programs for staff.

By implementing the recommendations in this report, DGH can achieve a more secure, GDPR compliant work organization, which will help them stand out under the compliance laws and avoid any damage.

REFERENCES

St James Hospital (2025) About Us. Available at: https://www.stjames.ie/aboutus/ (Accessed: 9 November 2025).

intersoft consulting (2025) Art. 4 GDPR Definitions. Available at: https://gdpr-info.eu/art-4-gdpr/ (Accessed: 9 November 2025)

Paubox2024), What is an electronic health record (EHR)?, Available at: https://www.paubox.com/blog/what-is-an-electronic-health-record-ehr (Accessed: 11 November 2025)

Thomson Reuters Practical Law (2025) Home Electronic Health Record (EHR). Available at: https://uk.practicallaw.thomsonreuters.com/5-502-5347?transitionType=Default&contextData=(sc.Default)&firstPage=true (Accessed: 11 November 2025)

intersoft consulting (2025) Art. 9 GDPR Processing of special categories of personal data. Available at: https://gdpr-info.eu/art-9-gdpr/ (Accessed: 11 November 2025)

intersoft consulting (2025) Art. 24 GDPR Responsibility of the controller. Available at: https://gdpr-info.eu/art-24-gdpr/ (Accessed: 11 November 2025)

Intersoft Consulting (2025) Art. 24 Art. 28 GDPR Processor. Available at: https://gdpr-info.eu/art-28-gdpr/ (Accessed: 11 November 2025)

Drdollah (2024) Network Architecture for Healthcare Information Systems https://drdollah.com/hospital-information-system-his/system-architecture/ (Accessed: 11 November 2025)

National Library of Medicine *National Center for Biotechnology Information* (No year) Health Data Processes: A Framework for Analyzing and Discussing Efficient Use and Reuse of Health Data With a Focus on Patient-Reported Outcome Measures https://pmc.ncbi.nlm.nih.gov/articles/PMC6547770/ (Accessed: 11 November 2025)

Intersoft Consulting (2025) GDPR Fines / Penalties. Available at: https://gdpr-info.eu/issues/fines-penalties/ (Accessed: 11 November 2025)

Privacy Engine (2023) Understanding Data Breaches: Answers to Your Top Questions about Incident Management. Available at: https://gdpr-info.eu/issues/fines-penalties/ (Accessed: 11 November 2025)

Comply Dog (2025) GDPR Compliance Checklist: Complete 2025 Guide for B2B SaaS Companies. Available at: https://complydog.com/blog/gdpr-compliance-checklist-complete-guide-b2b-saas-companies/ (Accessed: 14 November 2025)

Sprinto (2025) Achieving GDPR Compliance: A Guide for Businesses: Complete 2025 Guide for B2B SaaS Companies. Available at: https://sprinto.com/blog/gdpr-compliance/ (Accessed: 14 November 2025)