



Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

Data Security, Governance and Compliance

ACCA7028

Student Name : Jay Shaileshbhai Lad

Student ID:2504388

Program: MSc Cybersecurity and Digital Forensics

Submission To: Dr. Dipo Dunsin

Contents

1.Introduction.....	1
2.Background and Scenario Analysis	1
3.Threat Landscape & Risk Assessment.....	2
4.Governance & Compliance Requirements.....	3
5.Proposed Security Governance Framework.....	5
5.1 Governance Structure.....	5
5.2 Policies & Procedures	5
5.3 Framework of Data Classification.	6
5.4 Access Control Model.....	6
5.5 Technical Security Controls	6
5.6 Incident Response Framework.....	7
5.7 Training & Awareness	7
6. Implementation Roadmap.....	7
6.1 Short-Term Actions	7
6.2 Medium-Term Actions	8
6.3 Long-Term Actions	8
6.4 Implementation Risks & Mitigation	8
7. Recommendations.....	8
8. Conclusion	9
References.....	11

1.Introduction

In this report, it is shown that data security, governance, and compliance are very critical in the context of the National Health Service (NHS) as it is attempting a major digital transformation. With the increased use of electronic systems, cloud-providers, and digital platforms, which tie like a web together, healthcare organisations, the amount of patient data being processed has increased manifold. The change has come with significant advantages in patient care, efficiency, and data-driven decision-making but it has also created a broad spectrum of cybersecurity weaknesses and governance pitfalls. The NHS being one of the largest public sector organisations in the world deals with highly confidential medical information; hence it is an ideal target of cyberattacks and data breaches.

This report aims at assessing the present threat environment of NHS, examining its regulatory and governance responsibilities, and offering an elaborate security framework to suit its operational and regulatory needs. The report will present a systematic method of enhancing resiliency, lawfulness, and information management in general in NHS settings by incorporating the best practices like ISO 27001, NIST Cybersecurity Framework, as well as GDPR principles.

To do so, the report is organised into some major parts. It starts with the background overview of NHS scenario and the analysis of external and internal threats. It proceeds to analyze governance and compliance policies, propose a security governance model, and give an implementation plan. The report ends with strategic recommendations that are meant to facilitate the effective and secure digital transformation throughout the NHS.

2.Background and Scenario Analysis

National Health Service (NHS) is one of the most massive and intricate healthcare eco-systems in the world, which has been extensively dependent on digital technologies to aid in the provision of clinical care, administrative processes, and national health services. In hospitals, general practitioner practices, community clinics, and specialist centres, there are enormous volumes of digital health information that are gathered, stored and worked out using electronic health records, diagnostic systems, patient management systems and national databases. These inter-related systems will enhance efficiency, data sharing, evidence-based decision making,

and patient outcomes. Nevertheless, such high degree of interconnectivity is creating numerous points of vulnerability to cyber threats exposing the NHS to security breaches and operational disruption [8].

In the past, the NHS has been faced with immense cybersecurity issues. Among them, the most prominent cases are the ransomware attacks like WannaCry, where the old and unpatched systems were targeted in hundreds of Trusts and caused the closure of operations and widespread disruption of services [2]. The use of outdated technologies that are not provided with modern security measures among many NHS Trusts still exposes them to exploitation. Also, the policies of governance and security are not consistently applied throughout all Trusts and this leads to inconsistent security practices, few coordination and lack of accountability. The size and the variety of NHS operations render the implementation of uniform structures of governance, security measures, and risk management approaches challenging [3].

The situation exposes a number of fundamental challenges that need quick efforts to be resolved: growing reliance on online work, growing cyber risks against the healthcare sector, regulatory imperatives with GDPR and the Data Protection Act, and the necessity to establish a single model of security governance, which can be implemented in NHS settings [4]. These issues illustrate the reasons as to why NHS needs a holistic security governance framework that incorporates technical controls, procedural standards, legal compliance, and organisational accountability to provide digital healthcare delivery that is both resilient and secure.

3.Threat Landscape & Risk Assessment

The NHS is experiencing a wide and changing threat environment, which is influenced by their large-scale digital platform, the monetisation of health data, and the prevalence of interconnectivity between clinical infrastructures. The threat of external attacks is also a major issue, and in this case, advanced cyberattacks that affect healthcare organisations. Ransomware is also one of the most disruptive threats that can encrypt critical systems and stop the clinical workflow until the payment of a ransom. This is particularly susceptible in the healthcare sector that depends on the availability of the system on demand. Phishing is a frequent technique of delivery, with the intention of stealing or installing malware based on the use of deceptive emails, and can be taken up by the staff members, who might not be thoroughly informed on the issue of security threat. Moreover, distributed denial-of-service (DDoS) attacks and cyber

campaigns by nation-states only make the situation worse, with an attacker trying to gain access to sensitive data of patients, or hobble public services [9].

A human error is also the most prevalent cause of data breaches and it constitutes internal threats as well. Employees can unintentionally reveal customer data, incorrectly set up system parameters, or be the victims of the social engineering efforts. Confidentiality, integrity, or availability of NHS data may also be at risk by insider misuse (either by negligence or by ill intent). These risks are further increased by weak passwords, the lack of good access control, and the lack of adherence to data-handling practices, which underscores the importance of a strong internal security culture and governance [12] .

There are a number of systemic weaknesses that add the exposure to the NHS. Outdated software, which runs many of them, has no current security controls, and may not be regularly patched against security vulnerabilities [10]. This establishes easy vulnerabilities to the attackers. Different Trusts have fragmented governance that results in inconsistency in practices relating to security and ineffective risk management. Also, lack of adequate training and awareness of the staff lowers the capability of the organisation to identify and counter threats early enough.

Through data on a structured risk assessment, it can be indicated that a number of these threats are highly likely and impactful. The probability of ransomware, phishing, and data breaches is extremely low, given the size and publicity of the NHS, whereas its consequences might include the closure of its operations, jeopardized patient safety, fines in the context of GDPR, and negative publicity. Intra-organizational mistakes and flaws in governance are moderately probable though with an important repercussion. On the whole, NHS is at risk environment where the risks are critical requiring immediate, coordinated and strategic mitigation measures.

4.Governance & Compliance Requirements

The NHS is situated in a very high legal and regulatory atmosphere, which aims at preserving personal information and maintaining responsible data management. At the core of this infrastructure is the General Data Protection Regulation (GDPR) that establishes the most important principles including lawfulness, transparency, data minimisation, and accountability. The NHS under GDPR will need to show that the patient data is handled in a secure manner, with a defined set of valid purposes of use, and with a high level of control access. To

complement GDPR, the Data Protection Act (DPA) 2018 deploys the provisions of the UK context, establishing the national mechanisms of enforcement and other protection of sensitive health data. Violation of such regulations may lead to heavy fines, damaged reputation and lost patient confidence.

Besides the general data protection legislation, the NHS has to comply with the requirements that have been specific to the healthcare sector. The Data Security and Protection (DSP) Toolkit compels all NHS organisations and partners to review and disclose the data security and data governance practices annually. It offers a standardised way of assessing organisational preparedness, risk stance as well as compliance maturity. The Caldicott Principles that emphasize the ethical management of patient-identifiable information support the importance of justifiable access and use of personal data to the minimal extent. Every NHS Trust has to constitute a Caldicott Guardian who will supervise the observance of these principles and will keep the patient confidentiality as the priority [6].

In addition to legal and sector-specific controls, the NHS is in a way being pushed to align to the recognised industry standards to enhance its security posture. The ISO 27001 offers a powerful model to set up an Information Security Management System (ISMS), which has systematized procedures in risk assessment, policy formulation as well as continuous enhancement. The NIST Cybersecurity Framework (CSF) assists organisations to designate, shield against, identify, react to, and recuperate cyber threats. In the case of healthcare-specific requirements, ISO 27799 describes the requirements that are specific to protecting health information in a complex clinical setting.

Nonetheless, it is difficult to have proper governance throughout the NHS. The extremely decentralised structure of the organisation implies that individual Trusts have free will to manage their digital systems, policies, and functioning practices. This decentralisation tends to be associated with uneven security control, inconsistent policy adoption, disjointed risk management activities and differences in maturity levels of compliance. The old system and resource limitation also add pressure to the alignment with the national standards. The difficulties mentioned above underscore the importance of a unified and coordinated approach to governance that would guarantee a steady level of compliance, enhance accountability, and enhance resilience throughout the NHS [5].

5. Proposed Security Governance Framework

The NHS needs to have a strong and unified security governance model to enhance its capacity to safeguard confidential health data, meet legal obligations and achieve business continuity. All the specified framework incorporates organisational governance, technical protections, procedural standards, and cultural development to develop a comprehensive model that can be adopted throughout NHS Trusts [15].

5.1 Governance Structure

The governance should start with effective leadership and accountability. The implementation and design of security strategies should be led by a Chief Information Security Officer (CISO) who must ensure their compatibility with standards and guidelines in the NHS and future threats. A Data Protection Officer (DPO) is entitled with the statutory obligation of the GDPR and DPA 2018 compliance, carrying out impact analysis and tracking the data processing operations. The Information Governance (IG) Leads assist every Trust in executing security policies, risk assessment, and internal audits. Also, the Caldicott Guardian is a key figure in supporting patient-identifiable information confidentiality, as well as establishing that the sharing of data is reasonable, limited, and handled in an ethical manner. Taken together, these functions generate an orderly system of governance, which enhances responsibility and strategic control [7].

5.2 Policies & Procedures

Clear policies will be critical towards supporting safe conduct in the NHS workforce. Acceptable Use Policies set anticipated norms of computer systems and equipment utilization to aid in avoiding abuse and unintentional disclosure of information [14]. Access Control Policies are used to establish the manner in which rights and permission are established so that only a qualified individual accesses a certain information. Encryption Policies stipulate the application of authorised cryptographic controls over data data on rest and in transit, limiting the exposure to data interception or unauthorised access. Also, there is Data Retention and Disposal Policies that it is kept only at the required times and safely destroyed once not needed. These control procedures instil consistency and foster conformity in Trusts.

5.3 Framework of Data Classification.

An organized model data classification will help the NHS to secure information according to its sensitivity. Data can be grouped into four levels; Public, Internal, Confidential, and Highly Confidential, with the patient health records being classified under the highest level. Every classification has its rules of handling, such as the tightening of the access control, increasing the encryption, and implementing the secure transportation. This framework will help guarantee that sensitive data will be afforded maximum protection and allow sharing it to the greatest extent possible as needed to be shared in the name of clinical and operational purposes [11].

5.4 Access Control Model

The adoption of secure access model is essential in insider risks reduction and restricting unauthorised access to the system. The Zero Trust strategy presupposes that no devices or users can be trusted, as they should be verified and monitored on a regular basis. Role-Based Access Control (RBAC) will ensure that a person can only access data which is pertinent to their job functions and minimizes superfluous privileges which can be abused. Multi-Factor Authentication (MFA) requires the use of a strong security layer and it ensures account security despite the compromise of passwords. All these measures combined have a high probability of minimizing the vulnerability of unauthorised access [13].

5.5 Technical Security Controls

Technical safeguards present the technical basis in safeguarding the NHS systems. Encryption guarantees confidentiality, whereas a regular patching and management of vulnerability prevents the use of out-of-date software. Security Information and Event Management (SIEM) system allows real-time monitoring and threat detection and automatic alerts throughout the network. Network segmentation helps to reduce the diffusion of attacks by isolating important systems. Strong backup and recovery measures ensure integrity of the data and ensure the quick recovery following the cyber attacks. These technical controls are taken together to make the system more resilient.

5.6 Incident Response Framework

Planned incident response will guarantee quick and efficient response to security incidents. The eradication process gets rid of evil in the infected systems after which the recovery process that restores normalcy takes place [1]. Lastly, lessons learned are recorded and incorporated in future enhancements that would help in making organisations prepared.

5.7 Training & Awareness

The aspect of human behaviour is a crucial issue in cybersecurity. Periodic employee training will facilitate the knowledge of the employees about risks, policies and best practices. Awareness and safe behaviour can be checked with the help of simulated phishing exercises. The creation of a security-conscious culture imparts on the staff the need to identify threats, adhere to the process, and report the presence. Highly informed employees minimize human vulnerability greatly.

6. Implementation Roadmap

The implementation of security governance framework proposed requires gradual implementation with a road map to be put in place to ensure that the implementation is effective throughout the NHS (Salako et al., 2024). This is an organized strategy that helps Trusts to focus on important actions to take, resource mobilization, and other things that cause minimal disturbance to clinical and operational services. The roadmap has been broken down into short, middle and long term phases, which deal with particular organisational and technical requirements.

6.1 Short-Term Actions

The first stage is dedicated to setting up of baseline governance and security controls. Among the short-term priorities, there is the need to update the organisational policies to ensure their compliance with GDPR, the requirements of the DPA 2018, and the recently suggested security standards. Implementation of Multi-Factor Authentication (MFA) in all user accounts in the NHS must also take place at this phase since it will go a long way to mitigate the risks of unsanctioned accessibility. The baseline risk analysis helps Trusts to understand existing vulnerabilities, focus on remediation activities, and measure improvement progress in the

future. This initial action predetermines a steady state of security in Trusts and preconditions the further developed initiatives.

6.2 Medium-Term Actions

When the basis controls have been established, attention is paid to enhancing monitoring and technical defences. Implementation of the Security Information and Event Management (SIEM) tools will enable real time visibility of the possible threats and will be used to monitor the centralised incidents. Segmenting the network can assist in isolating the vital clinical systems, limiting the chances of attacking in the future, and also minimise the effect of any attack. Patching of legacy systems, hardening of systems, and implementation of secure configurations is further trimming of the exposure of exploitable vulnerabilities. It is a step that would make the NHS better placed to identify, contain, and respond to cyber threats.

6.3 Long-Term Actions

Operational efficiency and the provision of resources to strategic activity are ensured by the introduction of automation technologies, including automated patching, compliance reporting, and threat detection. Incorporation of ongoing governance controls means that you have a fixed review of policies, audit, and long-term observation of arising threats such that the NHS is in a robust security posture.

6.4 Implementation Risks & Mitigation

The challenges in implementation might include limitation of resources, resistance of staff to change, technical debt and integration with legacy systems. Several measures must be adopted in order to reduce these risks in the NHS; this includes a robust leadership role, allocate specific budgets, offer specific trainings, and employ a gradual implementation approach. A frequent appraisal and stakeholder involvement will also help to promote the successful implementation and sustainability of long-term security.

7. Recommendations

According to the conclusions drawn after analyzing the current digital environment of the NHS, the exposure to threats, and governance issues, one can offer several specific suggestions to contribute to the creation of the secure and resilient information management environment [16]. The top priority improvements are to be made on handling the vulnerabilities that are

immediate and especially that of access control and obsolete systems. The introduction of the mandatory Multi-Factor Authentication, fastening the patching rates, and decreasing the use of the old technologies will considerably decrease the probability of cyber attacks. The improvement in the centralised monitoring will also enhance the ability of the NHS to detect and respond to threats in real time.

To maintain the long term security gains, modernisation of infrastructure must be made through strategic investment. Investment in Security Information and Event Management (SIEM) systems, more sophisticated endpoint protection, data loss prevention technology, and cloud architecture will enhance the technical base of the NHS. Human vulnerabilities will be mitigated by investing in workforce development (training programmes, security awareness, and hiring of qualified cybersecurity experts) and enhancing organisational capacity.

The strengthening of governance should be geared towards implementing a similar set of roles, responsibilities, and reporting lines among all the NHS Trusts. The top-level controls over roles of the CISO, DPO, and Caldicott Guardian should be strengthened to have a structured decision-making and responsibility. A uniform governance structure will be used to minimise fragmentation and adoption of best practices.

Lastly, adherence should be an ongoing endeavour. NHS organisations ought to periodically review compliance with GDPR, Data Protection Act and Data Security and Protection Toolkit, and gradually incorporate international standards, including ISO 27001 and ISO 27799 [17]. keeping the regulation and upholding the compliance will not only minimize the regulatory risk but also foster the culture of safety and ethical data care throughout the whole NHS.

8. Conclusion

The case of the NHS in the digital environment demonstrates a complicated risk environment due to the growing number of cyber threats, the reliance of operations on interconnected systems, and old governance issues.

The suggested security governance framework will provide a holistic way of dealing with these issues. The framework will improve the capacity of the NHS to prevent sensitive information from being exposed to hackers, and help the organisation withstand the changing cyber threats by clarifying the leadership roles, standardising policies and procedures, introducing a structured data classification system, using a Zero Trust access model, and reinforcing the

technical defences. Both the technical and human factor is addressed since a sound incident response process and constant training is incorporated. The gradual implementation plan also facilitates the reasonable adoption of the plan at NHS Trusts, which makes the resource restrictions and work demands manageable.

Finally, this framework is directly aligned with the needs of the scenario in the NHS, as in the case, issues with fragmentation, old systems, and inconsistent governance have been impeding the efficiency of security. With a coordinated, holistic strategy in place, the NHS will be able to modernise its security posture, enhance compliance and facilitate a more secure and resilient digital healthcare ecosystem. This not only ensures the data of patients is safeguarded but it also empowers the people with their trust, not to mention making the digital transformation process sustainable and secure.

References

- [1] M. M. Ahmed, O. J. Okesanya, M. Oweidat, Z. K. Othman, S. S. Musa, and D. E. Lucero-Prisno III, “The ethics of data mining in healthcare: challenges, frameworks, and future directions,” *BioData Mining*, vol. 18, no. 1, Jul. 2025, doi: <https://doi.org/10.1186/s13040-025-00461-w>.
- [2] R. Aljuraid and T. Justinia, “Classification of Challenges and Threats in Healthcare Cybersecurity: A Systematic Review,” *Studies in health technology and informatics*, vol. 295, pp. 362–365, Jun. 2022, doi: <https://doi.org/10.3233/shti220739>.
- [3] W. Burke, A. Stranieri, T. Oseni, and I. Gondal, “The need for cybersecurity self-evaluation in healthcare,” *BMC Medical Informatics and Decision Making*, vol. 24, no. 1, pp. 1–15, May 2024, doi: <https://doi.org/10.1186/s12911-024-02551-x>.
- [4] C. Dameff *et al.*, “Ransomware Attack Associated With Disruptions at Adjacent Emergency Departments in the US,” *JAMA network open*, vol. 6, no. 5, p. e2312270, May 2023, doi: <https://doi.org/10.1001/jamanetworkopen.2023.12270>.
- [5] S. G. Heshajin, S. Sedghi, S. Panahi, and A. Takian, “A framework for health information governance: a scoping review,” *Health Research Policy and Systems*, vol. 22, no. 1, Aug. 2024, doi: <https://doi.org/10.1186/s12961-024-01193-9>.
- [6] Y. He, L. Maglaras, A. Aliyu, and C. Luo, “Healthcare Security Incident Response Strategy - A Proactive Incident Response (IR) Procedure,” *Security and Communication Networks*, vol. 2022, pp. 1–10, Feb. 2022, doi: <https://doi.org/10.1155/2022/2775249>.
- [7] N. L. Ngesimani, E. Ruhode, and P.-A. Harpur, “Data governance in healthcare information systems: A systematic literature review,” *SA Journal of Information Management*, vol. 24, no. 1, Aug. 2022, doi: <https://doi.org/10.4102/sajim.v24i1.1475>.

- [8] S. Nifakos *et al.*, “Influence of Human Factors on Cyber Security within Healthcare Organisations: A Systematic Review,” *Sensors*, vol. 21, no. 15, p. 5119, Jul. 2021, doi: <https://doi.org/10.3390/s21155119>.
- [9] O. Ogunwole, E. C. Onukwulu, M. O. Joel, E. M. Adaga, and A. I. Ibeh, “Modernizing Legacy Systems: A Scalable Approach to Next-Generation Data Architectures and Seamless Integration,” *International Journal of Multidisciplinary Research and Growth Evaluation.*, vol. 4, no. 1, pp. 901–909, 2023, Available: https://www.allmultidisciplinaryjournal.com/uploads/archives/20250306182550_MGE-2025-2-018.1.pdf
- [10] F. Rizzoni, S. Magalini, A. Casaroli, P. Mari, M. Dixon, and L. Coventry, “Phishing simulation exercise in a large hospital: A case study,” *DIGITAL HEALTH*, vol. 8, no. 1–13, p. 205520762210817, Jan. 2022, doi: <https://doi.org/10.1177/20552076221081716>.
- [11] A. O. Salako, Fabuyi, Jumai Adedoja, A. N. Taiwo, O. Selesi-Aina, D.-O. D. Louisa, and Olaniyi, Oluwaseun Oladeji, “Advancing Information Governance in AI-Driven Cloud Ecosystem: Strategies for Enhancing Data Security and Meeting Regulatory Compliance - ScienceOpen Library,” *Submanuscript.com*, Dec. 2024, doi: <http://journal.submanuscript.com/id/eprint/2644/1/Salako17122024AJRCOS127573.pdf>.
- [12] S. Smyth, “Penetration Testing and Legacy Systems,” *arXiv.org*, Dec. 17, 2023. <https://arxiv.org/abs/2402.10217>
- [13] A. J. Cartwright, “The elephant in the room: cybersecurity in healthcare,” *Journal of Clinical Monitoring and Computing*, vol. 37, no. 5, Apr. 2023, doi: <https://doi.org/10.1007/s10877-023-01013-5>.

- [14] “Cyberattacks and the Cybercrime Threat of Ransomware to Hospitals and Healthcare Services During the COVID-19 Pandemic | *Acta Criminologica : African Journal of Criminology & Victimology*,” *Acta Criminologica : African Journal of Criminology & Victimology*, 2021, doi: <https://doi.org/10.10520/crim.v34.n3;article:article:doi>.
- [15] N. Mohammed, A. F. Mohammed, and Sruthi Balammagary, “Ransomware in Healthcare: Reducing Threats to Patient Care,” *Journal of Cognitive Computing and Cybernetic Innovations*, vol. 1, no. 2, pp. 27–33, 2025, doi: <https://doi.org/10.21276/jccci.2025.v1.i2.5>.
- [16] B. Aldosari, “Cybersecurity in Healthcare: New Threat to Patient Safety,” *Cureus*, vol. 17, no. 5, May 2025, doi: <https://doi.org/10.7759/cureus.83614>.
- [17] F. Romolo, S. Grassi, A. Luca, M. Previtali, and A. Oliva, “Health and Cybercrime*,” *European Review of Digital Administration & Law -Erdal*, vol. 2023, no. 1, pp. 287–297, 2023, doi: <https://doi.org/10.53136/9791221811285>.