Contents

Introduction

This report will cover ISM practices relating to healthcare and, more specifically, the NHS. I will detail a selection of recent incidents in the healthcare sector and their potential Information Security Management implications. Using these examples, I will justify the need for improved ISM practices in the NHS and using this, will provide a list of assets, evaluate the risks associated and provide risk mitigation strategies to improve security in the NHS. By understanding real examples of failures in the recent past, we can evaluate where we are failing similarly and where the evidence shows we should be targeting.

In addition to the risk analysis, I will provide a security policy detailing where the gaps in the current security policies lie, and recommendations for improvements we can begin implementing. This policy will cover the roles and responsibilities within the business, best practices and rules that will ensure security remains a priority going forward. The importance of clearly defining aspects of this policy will ensure proven processes are followed in the event of an emergency and that the structure of business operations does not collapse during panic.

Linking in with the security policy, I will cover training recommendations in detail and how we can promote the new policy to ensure compliance with not only the legal aspects of security but also how we can be as compliant to the ISO 27001/27002 standards as possible to increase our preparedness for cyber threats.

In general, the report will focus more on the non-technical aspects of security, as this is where we can make very meaningful changes, as per the cyber security breaches survey[2] phishing attacks remain the most prevalent attack with 54% of businesses reporting a phishing-related breach, demonstrating the massive impact the human factor has on security.

Finally, I will detail relevant laws relating to security within the NHS. I will justify why assigning resources to complying with these laws is important and provide specific examples of laws and how we can comply with them.

The document will conclude with a section summarising the report and highlighting the main focuses of the document to reiterate their importance.

Analysis of the recent incidents

Synnovis attack

On the 3rd of June 2024, the company Synnovis, who provide pathology services (blood and urine tests) for hospitals in the NHS, were hit with a ransomware attack that caused delays to over 11,000 outpatient appointments[5] and had effects lasting until December 2024[5]. The lasting impact of this attack shows there were not sufficient disaster recovery plans in place to handle this sort of attack. The attack affected the company's IT systems, which had a long-lasting impact on their ability to manage patient data relating to tests. In addition to the IT services being affected by the attack, the attackers also leaked patient data on the 20th of June 2024[5]. Synnovis reported the incident to the Information Commissioner's Office, and according to Synnovis' official site[7], as of the 18th of December 2024, they were still looking into the details and the extent of the stolen data. During the period of technical outage, Synnovis resorted to paper processes, which they themselves admit significantly affected delivery timeframes and capacity to manage tests and other related processes[7] A lack of a comprehensive security policy may have impacted their ability to bring systems back online, which shows the importance of strong risk mitigation strategies and planning.

Ascension ransomware attack

In May 2024, Ascension Health was target to a ransomware attack in which over 5.5 million records were estimated to be affected. Initially, they were only aware of the ransomware attack, but later confirmed that information was also stolen. This attack had a lasting impact on Ascension health, leading to financial difficulties, service interruptions and taking IT infrastructure offline entirely[10]. Similar to other related attacks, Ascension were forced to resort to pen and paper for patient information, highlighting insufficient redundancy systems and an ill-preparedness to manage modern cyber threats, especially in an age where IT systems are so integrated into operations, whether that is a good or bad thing.

Addenbrooke Data leaks

In 2020 and 2021, two responses to a Freedom of Information Act request[14] contained patient information outside of the information that should have been sent. This incident occurred in the Cambridge hospital, "The Rosie Hospital", and included information relating to over 22,000 patients over a period of just over 2 years[12]. The requests were received through the site "What do they know?" which provides users a way to request data through their services so they can format and send the request on behalf of the user[15]. Sending data through an external service like this poses a serious non-technological security risk. Given the amount of time that passed before these data breaches were discovered, it is apparent that sufficient checks and security measures were not performed on both Addenbrooke and the What Do They Know service.

This breach highlights the importance of managing sensitive information internally as much as possible, and where external services are required, ensuring all security practices are of the same standard as would be expected internally.

Key outcomes

The healthcare sector has a trend of having poor ISM practices, especially when relating to the non-technical. As a trend, the healthcare sector often struggles with disaster recovery plans

and redundancy systems, often relying on pen and paper when an attack occurs, which does serve its purpose, however, a good disaster recovery plan might include air gapped redundancy servers and more technical backup systems to keep systems efficient, especially in an age of more Internet Of Things enabled devices. ISO 27002 recommends businesses to consider implementing redundant networks and two geographically separate data centres with mirrored systems[16] which would allow for less time outage if a ransomware or similar attack were to occur, however, this solution would not solve IT issues unrelated to data loss. For this reason, I will include other risk mitigation strategies in the following sections.

How this applies to the NHS

The example attacks above highlight the importance of the CIA triad (confidentiality, integrity and availability) in the healthcare sector. Confidentiality, more specifically GDPR compliance, helps us avoid fines that can be crippling to hospitals and cause an effect on patient assistance and health, as shown in the Ascension Health example, where the entire IT infrastructure was taken offline. A more immediate concern when it comes to the CIA triad is availability, as shown in these examples, resorting to pen and paper processes in a disaster event is a trend that the NHS cannot afford to rely on, Internet of things devices, like insulin pumps, patient monitors, messaging platforms on mobile devices rely on a consistent IT infrastructure and in a field where correct communication between humans and smart devices can be the difference between life and death, we can take these examples to show redundancy servers, correct training to minimise attack vectors for ransomware attacks must be improved to save lives.

Asset Inventory and Risk Analysis

ISO 27001[4]

Iso 27001 standards suggest organisations should conduct risk assessments that

- Detail acceptance criteria for a risk, as no risk can be truly removed, only mitigated
- Identifies the owners of a risk, who is responsible for managing that risk and who would be at fault if improperly managed
- The likelihood that a risk would occur
- Consequences of the risk
- Realistic likelihood that the risk would occur
- Compare the results after the risk management has been applied

I will aim to conduct my risk assessment in a way that complies with these guidelines.

Below is a list of assets. The table details the asset, the asset type (Physical, non-physical and personnel), a description of the asset, where it is located, who owns it and its impact on the business if it were to become unavailable.

Impact Key

This key provides context for what the different impact titles mean. This is not an assessment of risk, it only serves to show how important these assets are to the function of the business and which should therefore be prioritised and any risks associated with them be mitigated.

Impact	Context
None	No impact on NHS operations
Low impact	Minimal impact on operations. Quick to fix.
Medium Impact	Noticeable impact on NHS operations. May take longer to fix and not without interruption.
High impact	Very noticeable impact on NHS operation, affecting multiple other systems as well as its own, and taking sizable resources and time to fix
Critical impact	Causes NHS operations to cease. Takes undivided resources to fix.

Asset table

A list of assets in the NHS

Asset	Asset Type	Description	Location	Owner	Impact
Desktop PC	Physical	Desktop PC for accessing the internal system.	Offices	IT department	High impact
Insulin pumps	Physical	An Internet of Things-enabled device used to monitor glucose and insulin levels in patients	Portable. Attached to patients when in use.	NHS	High impact
MRI Machines	Physical	A medical device required to perform MRI scans	MRI labs	Radiology Department	High impact
Nursing staff	Personnel	Nursing staff	N/A	NHS	Critical
Doctors	Personnel	Doctor staff	N/A	NHS	Critical
IT staff	Personnel	IT staff	N/A	NHS	Critical
Tablets	Physical	A portable device used to access patient data without needing to move to a desktop terminal	Portable	IT Department	Medium Impact
Patient Medical Information	Non-Physical	Sensitive patient information	Servers	Patient and NHS	Critical
Staff information	Non-Physical	Sensitive Staff information	Servers	Staff member and NHS	High
Payroll information	Non-Physical	Payment information for staff members to receive their wage payments	Servers	Staff member and NHS	Medium Impact
Servers	Physical	Servers that house critical, sensitive and general information	Server Room	IT department	Critical
Patient Monitors	Physical	Monitors for viewing patient health, for example heartrate and blood pressure	Hospital rooms	NHS	Critical

Research information	Non-Physical	Sensitive research information is being conducted at a hospital within the NHS	Servers	Hospital, researcher and NHS	Medium Impact
Security cameras	Physical	Security cameras for physical security and legal evidence	Around the hospital buildings	Security	Low impact

---

		Severity				
		Insignificant	Minor	Moderate	Major	Critical
Likelihood	Very Unlikely	1	2	3	4	5
	Unlikely	2	4	6	8	10
	Possible	3	6	9	12	15
	Likely	4	8	12	16	20
	Almost Certain	5	10	15	20	25

The risk score is the severity multiplied by the likelihood of it occurring

Risk Score	Level	Description
1-4	Low	No changes necessary
5-9	Medium	Should be looked at for possible improvements
10-15	High	In need of immediate review
16-25	Critical	Immediately devote all resources to fixing

Risk Assessment

Risk	Risk Score	Mitigation(s)	Post mitigation Score	Justification
Servers go offline, meaning we cannot access patient data.	Severity = 5 Likelihood = 2 Score = 10 - High	Implement backup servers separate from the main network and located physically in a different area, so as not to have to rely on pen and paper.	Severity = 3 Likelihood = 2 Score = 6 – Medium	Servers going offline in a hospital will never be a completely smooth process, even with backup servers, the transition will not be seamless. In a hospital where every second can save a life, the impact of this event would still be severe.
Power outage	Severity = 5 Likelihood = 2 Score = 10 – High	Introduce backup generators that are set to take over when a power outage occurs. Ensure we draw power from a reliable power grid if possible	Severity = 3 Likelihood = 1 Score = 3 - Low	Applying these mitigations helps to reduce the impact of a power outage, but it's still only going to be for a limited time. Despite this, using these mitigations, we can be better prepared.
Patient monitors stop performing correctly	Severity = 5 Likelihood = 2 Score = 10 - High	Keep consistently tested spares. There should be enough to cover more than one at a time. When one is taken, replace it with a new one as quickly as possible.	Severity = 2 Likelihood = 2 Score = 4 - Low	This risk can be managed easily, so the severity score drops drastically. As long as they are replaced quickly, there will always be a flow of supply.
Research information leaked either through an attack or human error	Severity = 5 Likelihood = 3 Score = 15 - High	Ensure training to prevent the mishandling of data is required periodically, and we comply with the GDPR guidelines for data security.	Severity = 5 Likelihood = 2 Score = 10 - High	Due to the very sensitive nature and the financial implications of the research, there is no circumstance where this risk can be mitigated to the point where we no longer think about it. GDPR complicity is something we will need to consider every time we use the systems in the NHS
Patient information leaked	Severity = 5 Likelihood = 4 Score = 20 – Critical	Implement harsher staff training policies to help outline what information is protected and the methods attackers may use to gain access to that information (phishing, etc).	Severity = 5 Likelihood = 2 Score = 10 - High	The potential fines and their impact on the business mean the severity of an incident like this will always be critical.

Information Security Policy NHS

Scope

This information security policy applies to all assets of the NHS, physical or non-physical, including but not limited to the following:

- Staff employed by the NHS
- Data owned by the NHS
- Data managed by the NHS
- Internet-enabled devices on the NHS network
- Servers and datacentres managed or used by the NHS

Security Standard

The security policy is centred around General Data Protection Regulation (GDPR) compliance and ensuring data confidentiality, Integrity and availability is preserved. In addition to complying with legal requirements, we promise to uphold ISO 27001[4] standards relating to data security, risk management and asset management.

Usage policies

By using NHS information services, you must agree to uphold the following principles based on GDPR and ISO 27000 compliance:

- Do not open attachments from email senders you do not recognise and always report suspicious email activity
- Do not send sensitive company information to recipients outside of the NHS, and always refer to company access lists in order to see who is allowed to view information
- Do not attempt to access information higher than your allocated authority, whether this be physical documentation or computer systems.
- If you gain access to information you should not have access to, immediately report this incident to the relevant authority. For staff, this would be your direct supervisor. For patients and other visitors, please find the closest member of staff, and they will direct you.
- In general, report any suspicious or unusual activity to your direct supervisor.
- Any passwords used to access NHS systems must be changed to a unique password following the latest security standards at least once every 30 days
- All accounts must use at least two-factor verification (Phone number and/or authenticator)
- Staff must complete all mandatory legal compliance training before the deadline.

Roles and responsibilities

The following is a list of roles and their responsibilities for ensuring information security:

IT department – Manage computing and electronic devices to maintain GDPR compliance and general operational security (software updates, managing hardware vulnerabilities).

General NHS staff – Complying with usage policies.

Training and Awareness Plan

Phishing simulations

The cyber security breaches survey 2025[2] showed that 54% of businesses suffered a phishing related attack, making it the most common attack vector for gaining sensitive and valuable information. To combat this, phishing simulations will be sent to staff members periodically with the goal being staff members will learn to detect increasingly complex phishing emails, and report them for our dedicated IT staff to review and approve or deny.

An example email may contain a data request from a seemingly internal email address, this request may include requests for information unrelated to the job role of the recipient, or sensitive information that previous staff training would have outlined as targets for attackers and not to be sent over email. It is imperative for this type of simulation that the target never makes it as far as inputting information, as this would be a huge security risk, the link in the simulation should simply take them to a landing page that mentions they failed and auto-enrol them in more phishing training. If a staff member were to fail one of these simulations or not report them in a timely manner or at all, in addition to more training, they should receive a greater quantity of these simulations until they are consistently successful.

Phishing is such a prevalent issue in modern businesses, and it relies on the non-technical human factor, meaning risk analysis and risk mitigation measures are only as effective as staff understanding.

Gamified E - Learning

As mentioned in the phishing simulation, we will be applying E learning training, however, this will function differently from existing E learning solutions. E learning processes are fundamental to business training, but they are often uninteresting and therefore hard to engage with for general staff. Staff members don't like to stray from what's convenient to learn new systems and practices[18] To combat this, we can apply gamified e learning systems. Some suggestions for how this type of system may work are as follows:

- Quizzes based on the taught content in the E learning slides
- Scoring systems (e.g., points)
- Score incentives, for example, extra paid time off for top performers.
- Interactive slideshows, puzzles based around the taught content for example
- Group learning sessions.

The importance of staff understanding the training they receive is paramount to the success of the new security policy. Training is mandatory to ensure legal compliance but we don't want the training to feel like a roadblock staff members have to overcome, by adding incentives and dedicating paid time to completing E learning we can maximise the retention of information. One negative to adding gamified training could be the time impact, as we are aware from previous analysis, a small disruption to processes can have a massive impact on efficiency within the NHS, however, the consequences of mismanaging sensitive information, not complying with the security policies we have carefully selected for the purpose of safety are far greater than the time and money it would take to pay for and implement these gamified learning sessions.

Who we will train and what we will train them

Below is a table that highlights some of the main training areas and the staff the training applies to.

Green = Will receive training as it is relevant

Red = Will not receive training for one or more of the following reasons

- Not relevant to the job role
- Does not interact with that system / does not have permission to do so

Training Type	IT staff	General Staff	Managing staff
Phishing training			
Database security practices to comply with our established guidelines and processes			
General GDPR training			
Password standards training			
Passkey training (Physical passkey instead of password, IT staff may need quick access to systems. Usually works via NFC)			
2-factor authentication training			
Risk management training			

To increase awareness, we will send out company-wide emails and ask managers to describe and remind staff of the changes. As relying on staff to report back their contributions may not be accurate, we will also implement a mandatory usage policy that employees will have to sign and declare that they have read in order to access company systems. This policy will not contain strict details on how they should use the systems, but this one will serve the purpose of ensuring they understand how the new training systems work, and the minimum amount they will need to engage with the training, GDPR compliance training, etc.

Consideration and analysis of relevant laws

GDPR

The General Data Protection Regulation is a set of regulations that govern how to protect and manage sensitive information. In any organisation, this is the main data protection law. In the case of the NHS, ensuring we comply with the latest technical standards is something we will already be doing, a more relevant focus is the non-technical side of this legislation. To comply with GDPR[8], we must enforce the phishing and e learning training mentioned earlier in the document, by doing so we can minimise the possibility of the human factor causing a security breach.

Consequences for failing to comply with GDPR include fines, loss of business licence and legal prosecution, which, as mentioned previously, can be crippling for hospitals under the NHS, being a government-adjacent organisation does not exempt them from the consequences of a GDPR breach, especially if this breach is significant enough.

NIS

As the United Kingdom still does a large amount of trading with the European Union, whether that be physical assets or digital, even after leaving the Union, we should aim to comply with the Network and Information Systems Regulations (NIS), which are the European standards for information security adapted into UK law to remain compliant with EU standards[17]. NIS focuses on essential services and organisations that are deemed critical infrastructure, organisations that, if they were to fail, would have a meaningful impact on the country's economy. The NHS fits perfectly into this bracket, if NHS operations were to cease, the country's health would fall drastically.

As previously covered, by complying with GDPR and basing our security policies around the ISO 27000 series standards, we can minimise the impact of a disaster event and keep our critical assets running.

Conclusion

The outcome of the report can be summarised as an analysis of recent attacks in the medical field and their non-technical causes and implications. Using this analysis we determined what our critical assets are, physical and non-physical and applied risk management and mitigation strategies to minimise the impact they would have on NHS operations if they were to fail.

The main take away from this assessment is not to understate the importance and the reliance we have on technical systems in medicine, we must take a step back and consider just how much interconnectivity we use in modern-day medicine, like glucose monitors, and plan for how operations would work without the main systems we rely on.

Following the risk analysis, a one page information security policy was drafted to highlight some of the main points established in the previous sections and using this policy, a more detailed training and awareness plan was created, focusing on improving staff training through gamification methods and creating targeted phishing simulations to keep staff members practised and ready to face social engineering attacks.

Finally, we considered the relevant laws that apply to the NHS and how our plan aims to comply with the laws and mitigate risks associated with information security.

The overall message this report aimed to highlight is how important the non-technical side of security is. The human factor should not be understated and it is the responsibility of cybersecurity experts to not only educate staff but to do so in a way that does not confuse.

Reference list

(1) Computer Misuse Act (1990). *Computer Misuse Act 1990*. [online] Legislation.gov.uk. Available at: https://www.legislation.gov.uk/ukpga/1990/18/contents.

(2) Government of the UK (2025). *Cyber security breaches survey 2025*. [online] GOV.UK. Available at: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/cyber-security-breaches-survey-2025.

(3) Europa.eu. (2016). *EUR-Lex - 32016L1148 - EN - EUR-Lex*. [online] Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L1148.

(4) British Standards Institution (2023). *Expert Commentary for BS ISO/IEC 27001:2022. Information Security, Cybersecurity and Privacy Protection. Information Security Management Systems. Requirements*.

(5) www.england.nhs.uk. (n.d.). *NHS England» Synnovis cyber incident*. [online] Available at: https://www.england.nhs.uk/synnovis-cyber-incident/.

(6) Warren, J. (2025). NHS ransomware attack contributed to patient's death. *BBC News*. [online] 25 Jun. Available at: https://www.bbc.co.uk/news/articles/cp3ly4v2kp2o.

(7) Synnovis (2024). *Cyber Attack Information Centre*. [online] Synnovis. Available at: https://www.synnovis.co.uk/cyberattack-information-centre

(8) UK Government (2018). *UK General Data Protection Regulation*. [online] legislation.gov.uk. Available at: https://www.legislation.gov.uk/eur/2016/679/contents.

(9) European Commission (2023). *Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive) | Shaping Europe's digital future*. [online] digital-strategy.ec.europa.eu. Available at: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive.

(10) Alder, S. (2024). *Ascension Ransomware Attack: Initial Access Vector and Data Theft Confirmed*. [online] The HIPAA Journal. Available at: https://www.hipaajournal.com/ascension-cyberattack-2024/.

(11) Johnson, L. (2024). *Ascension Ransomware Attack: 5.6 Million Patients Affected - The HIPAA Guide*. [online] The HIPAA Guide. Available at: https://www.hipaaguide.net/ascension-ransomware-attack/

(12) Cambridge University Hospitals. (n.d.). *Statement from Roland Sinker, Chief Executive, Cambridge University Hospitals NHS Foundation Trust*. [online] Available at: https://www.cuh.nhs.uk/news/datastatement-6-december-2023/

(13) Issimdar, M. and Fox, N. (2023). Data breach by Addenbrooke's Hospital reveals patient information. *BBC News*. [online] 6 Dec. Available at: https://www.bbc.co.uk/news/uk-england-cambridgeshire-67639234.

(14) Gov.uk (2000). *Freedom of Information Act 2000*. [online] Legislation.gov.uk. Available at: https://www.legislation.gov.uk/ukpga/2000/36/contents.

(15) WhatDoTheyKnow. (2019). *Make and browse Freedom of Information (FOI) requests*. [online] Available at: https://www.whatdotheyknow.com/.

(16) British Standards Institution (2021). *BS ISO/IEC 27002. Information Security, Cybersecurity and Privacy Protection. Information Security Controls*.

(17) Legislation.gov.uk. (2018). *The Network and Information Systems Regulations 2018*. [online] Available at: https://www.legislation.gov.uk/uksi/2018/506/regulation/1.

(18) Bhosale, K.S., Nenova, M. and Iliev, G. (2021). A study of cyber attacks: In the healthcare sector. [online] IEEE Xplore. doi:https://doi.org/10.1109/Lighting49406.2021.9598947.

Student Declaration of AI Tool use in this Assessment

Please indicate your level of usage of generative AI for this assessment - please tick the appropriate category(s).

If the "Assisted Work" or "Partnered Work" category is selected, please expand on the usage and in which elements of the assignment the usage refers to.

Solo Work	**S1 - Generative AI tools have not been used for this assessment.**	☐
Assisted Work	**A1 – Idea Generation and Problem Exploration** Used to generate project ideas, explore different approaches to solving a problem, or suggest features for software or systems. Students must critically assess AI-generated suggestions and ensure their own intellectual contributions are central.	☐
	A2 - Planning & Structuring Projects AI may help outline the structure of reports, documentation and projects. The final structure and implementation must be the student's own work.	☐
	A3 – Code Architecture AI tools maybe used to help outline code architecture (e.g. suggesting class hierarchies or module breakdowns). The final code structure must be the student's own work.	☐
	A4 – Research Assistance Used to locate and summarise relevant articles, academic papers, technical documentation, or online resources (e.g. Stack Overflow, GitHub discussions. The interpretation and integration of research into the assignment remain the student's responsibility.	☐
	A5 - Language Refinement Used to check grammar, refine language, improve sentence structure in documentation not code. AI should be used only to provide suggestions for improvement. Students must ensure that the documentation accurately reflects the code and is technically correct.	☒
	A6 – Code Review AI tools can be used to check comments within the code and to suggest improvements to code readability, structure or syntax. AI should be used only to provide suggestions for improvement. Students must ensure that the code accurately reflects their knowledge and is technically correct.	☐
	A7 - Code Generation for Learning Purposes Used to generate example code snippets to understand syntax, explore alternative implementations, or learn new programming paradigms. Students must not submit AI-generated code as their own and must be able to explain how it works.	☐
	A8 - Technical Guidance & Debugging Support AI tools can be used to explain algorithms, programming concepts, or debugging strategies. Students may also help interpret error messages or	☐

	suggest possible fixes. However, students must write, test, and debug their own code independently and understand all solutions submitted.	
	A9 - Testing and Validation Support AI may assist in generating test cases, validating outputs, or suggesting edge cases for software testing. Students are responsible for designing comprehensive test plans and interpreting test results.	☐
	A10 - Data Analysis and Visualization Guidance AI tools can help suggest ways to analyse datasets or visualize results (e.g. recommending chart types or statistical methods). Students must perform the analysis themselves and understand the implications of the results.	☐
	A11 - Other uses not listed above Please specify:	☐
Partnered Work	**P1 - Generative AI tool usage has been used integrally for this assessment** Students can adopt approaches that are compliant with instructions in the assessment brief. Please Specify:	☐

Please provide details of AI usage and which elements of the coursework this relates to:
Used to check for spelling errors.

I understand that the ownership and responsibility for the academic integrity of this submitted assessment falls with me, the student.	☒
I confirm that all details provide above are an accurate description of how AI was used for this assessment.	☒