

LEVEL 4 ASSESSMENT



Module Name: *Networks and Cyber Security Essentials*



Module code: *ACCA4024*



Student name: *Thomas Pereira*



Student ID: *2442400*



Group: *1*



Lecturer's Name: *Amit Naik*



Submission: 30 April 2026

Executive Summary.....	3
1. Introduction.....	4
2. Identifying the Threats	5
2.1 External Threats.....	5
2.2 Internal Threats.....	6
3. Security Policies	7
3.1 Access Control Policy.....	7
3.2 Data Classification Policy	7
3.3 BYOD (Bring Your Own Device) Policy.....	7
3.4 Incident Response Policy	7
3.5 Password Policy.....	7
3.6 Acceptable Use Policy.....	8
4. Mitigation Measures.....	9
4.1 Multi-Factor Authentication (MFA)	9
4.2 Endpoint Detection and Response (EDR)	9
4.3 Cloud Security Checks (CSPM)	9
4.4 Network Segmentation and Zero Trust.....	9
4.5 Regular Backups.....	10
4.6 Keeping Systems Up to Date	10
4.7 Data Loss Prevention (DLP).....	10
5. Monitoring and Incident Response.....	11
5.1 Monitoring	11
5.2 Incident Response Plan	11
6. Staff Training and Awareness	13
6.1 Mandatory Annual Training.....	13
6.2 Fake Phishing Emails.....	13
6.3 Training for Specific Roles.....	13
6.4 Training for New Starters.....	13
6.5 Keeping Security in Mind Day-to-Day.....	13
7. Conclusion.....	14
8. References	15
9. Appendix A	17



Executive Summary

HealthPlus Analytics (HPA) is responsible for the processing of patient data at several hospitals and clinics in the United Kingdom in an environment that is highly prone to threats. The recent events that include unauthorised access to the patient data stored on the clouds and the infection of their analytics servers with ransomware have highlighted the vulnerability of their security measures. This report aims to establish a holistic framework for the security of data and governance to mitigate the impact of the above incidents and create a culture of security awareness. [1] [2]

The framework incorporates recognized international standards, such as ISO 27001 [3], NIST CSF (NIST Cybersecurity Framework) [4], and CIA triad (Confidentiality, Integrity, and Availability). It includes five main elements, which are threat identification, security policy, mitigation strategy, monitoring and incident response, and staff training.

1. Introduction

The health care sector is another industry that attracts more cyber attacks than any other [7] Patient data is very valuable as they can be sold to anyone on the dark web. Furthermore, the sector is always under time pressure to bring its system back online due to patient safety concerns.

The situation facing HPA is further complicated by the issue of several employees working from remote locations and using personal computers when accessing their company's information systems. This has complicated efforts towards securing the data. Recent breaches in security at HPA highlight the inadequacy of current measures and an urgent need for change.

This report focuses on the following five main points: threat assessment, development of appropriate security policies, implementation of necessary preventive actions, development of a monitoring and responding process, and training of the personnel. The main purpose of the report is to provide the board of directors with relevant information and recommendations.

The presentation of the above-listed findings to the board of directors can be found in Appendix A below.

2. Identifying the Threats

In order for us to solve the problem, we first need to determine the exact nature of the threat that HPA faces. There are basically two kinds of threats. These include threats coming from the external environment, as well as internal threats.

2.1 External Threats

External threats come from attackers outside the organization. These are the most visible risks and include:

Threat	What it means for HPA
Ransomware	Attackers lock the company's files and demand money to unlock them. HPA has already been hit by this and it caused significant disruption.
Phishing emails	Fake emails designed to trick staff into clicking dangerous links or giving away their passwords. Healthcare staff are frequently targeted.
Cloud misconfiguration	When cloud storage is not set up properly, it can be accessed by unauthorised people. This is what led to the patient data breach at HPA.
Advanced Persistent Threats	Organised, long-term attacks by criminal groups or state actors trying to steal data quietly without being detected.
Supply chain attacks	Attackers targeting third-party software or suppliers that HPA trusts, using that access to get into HPA systems.
DDoS attacks	Flooding HPA's systems with fake traffic to make them crash or go offline, disrupting access to patient data services.

2.2 Internal Threats

Internal threats come from people inside the company. These are often overlooked but can cause just as much damage as external attacks.

Threat	What it means for HPA
Malicious insider	An employee or contractor who deliberately steals or leaks patient data, often for personal financial gain.
Accidental mistakes	Staff using weak passwords, clicking phishing links, or accidentally sending sensitive data to the wrong person. These are very common and very costly.
Too much access	Employees who have more access to systems than they actually need. If their account is compromised, the damage is much worse.
Shadow IT	Staff using personal apps or cloud services (like personal Dropbox or Gmail) to store or share work data, bypassing company security controls.
Physical security	Someone walking into a server room or picking up a printed patient report left on a desk. Physical access is often overlooked.

Threats may affect all three components of the CIA Triad: Confidentiality (assuring that information remains private); Integrity (verifying that information has not been altered); and Availability (ensuring that systems function as required). All three must be covered by any HPA security architecture. [4] [3].

3. Security Policies

To address such risks, HPA requires a set of documented policies known to everyone. Without policies, no matter how efficient technologies will be implemented, nothing can be achieved since employees will not be aware of expectations from them. Listed below are the policies developed according to the ISO 27001 and UK GDPR guidelines.

3.1 Access Control Policy

However, everyone at HPA does not necessarily require access to all data. First and foremost, access should be granted according to the principle of least privilege, which suggests that users should be granted access to those resources that are essential for completing their tasks, but never to more. Secondly, all employees will have to use multi-factor authentication, which implies that a simple password would not be enough to log on to the network [3].

3.2 Data Classification Policy

All HPA's data should be classified as one of four types – Public, Internal, Confidential, and Restricted. Restricted includes patient data and needs to be protected by default – meaning it should be encrypted whether stored or transmitted. Employees need to be prevented from storing restricted data in personal computers or in any personal online cloud storage. This directly ensures compliance with UK GDPR Articles 5 and 32 [1].

3.3 BYOD (Bring Your Own Device) Policy

Most employees of HPA use their own devices such as mobile phones and laptops to do the tasks at HPA. The above-stated practice is acceptable but needs proper management. Only devices that use approved security applications which are capable of locking the device and deleting all data on the device in case of loss or theft must be allowed to access HPA's system. Jailbroken devices or rooted devices cannot be allowed into HPA's system.

3.4 Incident Response Policy

In case of any issues, there should be clarity regarding what action needs to be taken and within what timeframe. It is mandatory for all employees to report their observations of any potential security breach to the IT Security Team within an hour of discovering the situation. According to Article 33 of the UK GDPR, in case of any data breach involving patient data, the Information Commissioner's Office (ICO) should be notified within 72 hours [1]. HPA should maintain a record of all incidents and conduct post-incident reviews.

3.5 Password Policy

Password security is still a significant vulnerability for any organization. The minimum number of characters in an HPA password policy needs to be 14, using alphabets, digits, and special characters. Passwords should not be shared between users nor should be reused on other platforms. Users should change their passwords every three months. All employees need to use a password manager tool provided by the organization.

3.6 Acceptable Use Policy

The policy establishes general guidelines for HPA system usage: they are for business use only, no unauthorized software may be installed, and monitoring of computer activity will take place. Violation of this policy may result in disciplinary measures. It seems obvious enough yet documenting this and having all employees sign off on it is crucial from a legal standpoint.

4. Mitigation Measures

Policies on their own are not enough — HPA also needs to put practical technical and operational measures in place. The following measures directly address the threats identified in Section 2.

4.1 Multi-Factor Authentication (MFA)

One of the single most effective things that HPA can do is MFA. This is because even when attackers manage to get a person's password, they will not be able to log into accounts until they go through a second verification step which is usually a code sent to their mobile phones via apps. It should be enabled in all cloud services and remote logins immediately. Text messages are a big no-no here.

4.2 Endpoint Detection and Response (EDR)

The EDR software is installed on every system within the network of HPA and constantly monitors its activities. In the event that the ransomware starts encrypting the files, the software automatically halts the threat from spreading further. The appropriate tools to achieve this objective include CrowdStrike Falcon and Microsoft Defender for Endpoint. This recommendation directly addresses the problem of the ransomware attack that has been experienced by HPA.

4.3 Cloud Security Checks (CSPM)

The unauthorised access to the information at the HPA occurred due to a flaw in how the cloud-based storage was configured. A CSPM solution is an automated way to detect misconfigurations in the cloud infrastructure. These include having a storage bucket open to public view or user privileges exceeding their requirements. It can be expected that using such a solution would have detected the problem before any attacker discovered it.

4.4 Network Segmentation and Zero Trust

High Potential Acquirers should isolate their most critical assets such as those containing confidential patient information from the rest of their company network. Even within the corporate network, trust should not be presumed on either the device or individual level; each access attempt must be authenticated. This concept is called Zero Trust and is becoming more prevalent within NCSC guidelines [6] . Its primary advantage lies in limiting the ability of the attacker to navigate throughout the whole network if they do manage to break in.

4.5 Regular Backups

A good backup plan is the best protection from ransomware. HPA needs to practice the 3-2-1 method: maintain three backups of its data, store them in two kinds of media, and keep one backup completely disconnected from the system. It's important to test the backup solution monthly to ensure that it works. This would have significantly shortened the duration of recovery if such a plan were in place before the attack.

4.6 Keeping Systems Up to Date

Many attacks on networks exploit weaknesses in the software, which is not patched against such weaknesses. HPA requires a proper mechanism for patching its systems. It is essential that critical patches should be applied in two days after the availability of the patches [6]. Proper vulnerability scans should be performed regularly.

4.7 Data Loss Prevention (DLP)

The use of DLP technologies ensures that the communication channels for emails, file transfers, and cloud-based uploads are monitored to prevent the unauthorised transfer of patient data outside the organisation. For instance, in the case of an email containing unencrypted patient data in a spreadsheet form, the DLP technology will block such an email from being sent out.

5. Monitoring and Incident Response

Even with all the right policies and tools in place, things can still go wrong. That is why HPA needs a clear plan for monitoring its systems on an ongoing basis, and for responding quickly and effectively when an incident occurs.

5.1 Monitoring

A SIEM system is necessary for HPA as it provides a kind of dashboard that captures security alarms from all kinds of systems at one place. This should cover things like:

Failed login attempts, abnormal download of large amount of data, change in security configurations, and privileged user activity outside regular business hours [5] [6]

5.2 Incident Response Plan

When something does go wrong, everyone needs to know what to do. Based on the NIST SP 800-61 incident response framework, here is the step-by-step process recommended for HPA:

Step	What to do
1 — Detect	An alert is triggered by the SIEM system, the EDR tool, or a member of staff reporting something suspicious.
2 — Triage	The IT Security team quickly assesses how serious it is. Is it a critical breach or a minor alert? This determines the speed of the response.
3 — Contain	Affected systems are isolated. Compromised accounts are locked. Any known malicious connections are blocked immediately.
4 — Notify	If patient data is involved, the ICO must be notified within 72 hours under UK GDPR Article 33. Affected hospitals or clinics may also need to be informed.
5 — Eradicate	The root cause is removed — malware deleted, vulnerabilities patched, compromised accounts reset.
6 — Recover	Systems are restored from clean backups. Normal operations resume. Data integrity is confirmed before returning to service.
7 — Review	A post-incident meeting is held. What went wrong? What can be improved? Findings should update policies and training.

Critical incidents should be contained within four hours. High severity incidents within 24 hours. It is also worth considering a retainer with a specialist cybersecurity firm who can be called in for major breaches — this is particularly relevant given the sensitivity of the patient data HPA holds.

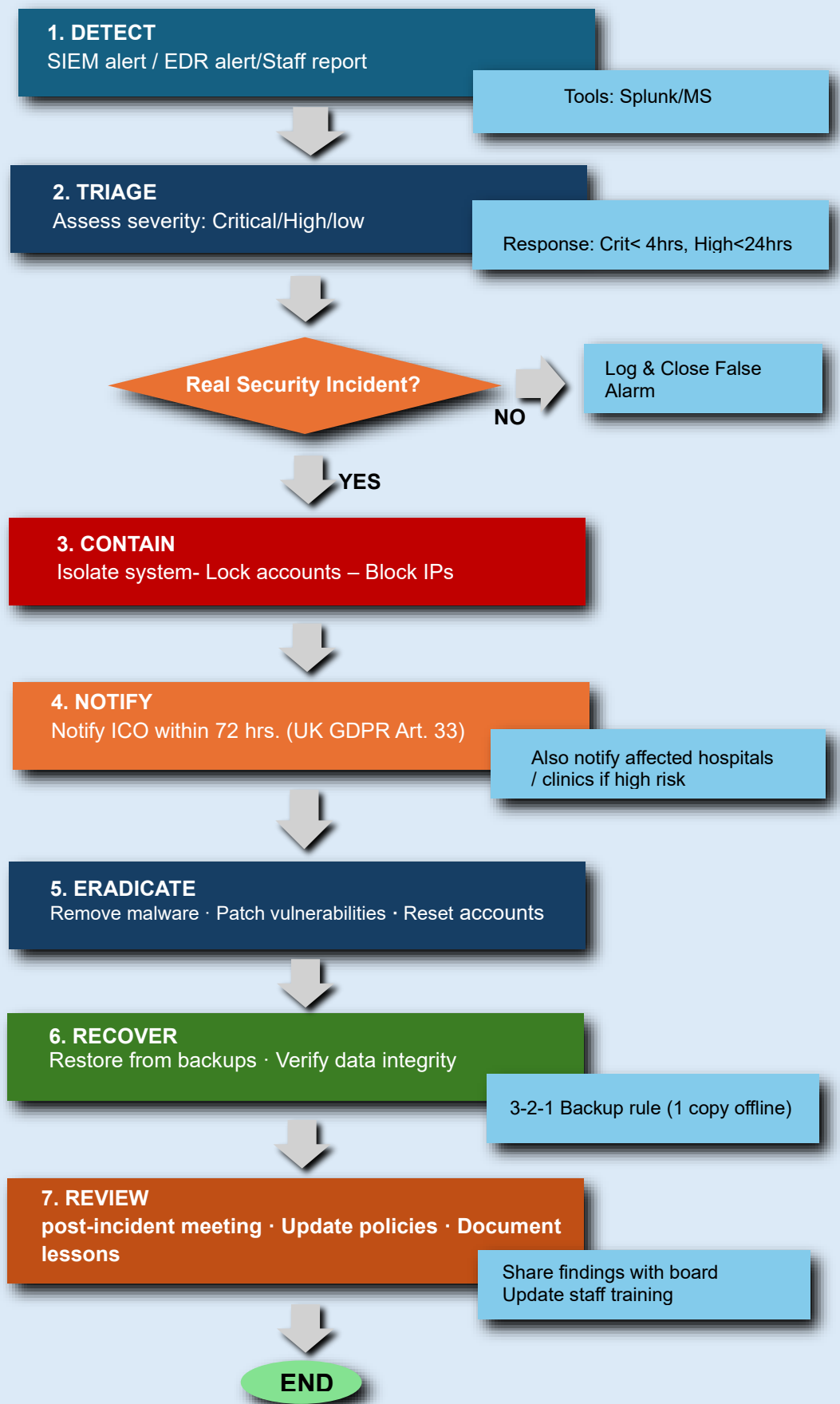


Fig 1: HPA Incident Response Flowchart (NIST SP 800-61)

6. Staff Training and Awareness

Cyber-attacks almost always begin as a result of human mistake – by clicking on an unauthorised email link, utilizing weak passwords, or emailing information to the incorrect recipient. Technology can only achieve so much. Human knowledge is equally crucial to technology. HPA is bound to follow certain regulations regarding training staff as per the NHS Data Security and Protection Toolkit [1] and UK GDPR [1].

6.1 Mandatory Annual Training

Every member of HPA should attend an annual online security awareness training program. The training session should include the following: how to detect phishing emails; how to securely store patient information; how to utilize multi-factor authentication and set up complex passwords; steps to take if there is a security breach, and key company policies. It is imperative to record completion of such training programs. If one does not complete it, he/she should be alerted by his/her superior officer. KnowBe4 and Proofpoint Security Awareness Training are great platforms for this.

6.2 Fake Phishing Emails

A phishing simulation should be sent once a month by the IT Security department to all employees. It would be a phishing email that looks realistic but is, in fact, part of the exercise. The user will be automatically directed to an educational module that teaches them what they missed. These simulations make the training more practical because it involves real-life scenarios. NHS England discovered that phishing simulations conducted on a monthly basis can reduce the number of victims by up to 70% in one year. [1]

6.3 Training for Specific Roles

HPA's employees do not all face the same security threats. Those who handle the company's IT systems and have administrative access require special training on topics such as cloud security and privileged account management. Developers should receive secure programming training based on the OWASP Top 10 [8]. The finance and HR departments are common targets of BEC attacks, which means they also require training.

6.4 Training for New Starters

New employees should complete security training before they are given access to any HPA systems. During their first week, they should be briefed on how to handle data, what the BYOD policy means in practice, and how to report an incident. They must sign the Acceptable Use Policy before access is granted.

6.5 Keeping Security in Mind Day-to-Day

Training once a year will not suffice alone. An individual in the HPA team should be nominated as the security champion who watches for undesirable practices and promotes desirable practices. Monthly newsletters focusing on cybersecurity could include items such as recent scam cases and tips on passwords hygiene. It is important to have an anonymous channel where employees can raise their concerns about any observation that may have been made

7. Conclusion

The situation at HPA could not be any worse. The information about the patients is extremely confidential and attractive to hackers; however, as is clear from the two most recent cases – namely, the ransomware attack and the breach of information on the cloud server – the security system currently utilized by HPA is clearly unable to protect against such situations. Luckily enough, though, both of the above-mentioned breaches were avoidable.

This proposed model does not require large investments or extremely complicated systems. The vast majority of near-term priorities – enabling MFA, adopting EDR, conducting phishing exercises – are simple and inexpensive solutions. What is required most of all is the willingness of the board to treat security as a priority and allocate funds for it appropriately.

In the long run, the objective must be to foster an environment where each employee realizes their responsibility for safeguarding personal health data – not only the IT department. Only then can HPA achieve true cybersecurity – and not just compliance.

8. References

- [1] Information Commissioner's Office (ICO). (2024). Guide to the UK General Data Protection Regulation. [Online]. Available at: ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources [Accessed: 30 April 2026]
- [2] National Institute of Standards and Technology (NIST). (2018). Cybersecurity Framework v1.1. [Online]. Available at: nist.gov/cyberframework [Accessed: 30 April 2026]
- [3] International Organisation for Standardisation. (2022). ISO/IEC 27001:2022 – Information Security Management. [Online]. Available at: iso.org/standard/27001 [Accessed: 30 April 2026]
- [4] NHS England. (2023). Data Security and Protection Toolkit. [Online]. Available at: dsptoolkit.nhs.uk [Accessed: 30 April 2026]
- [5] National Cyber Security Centre (NCSC). (2024). Ransomware: What it is and how to stay protected. [Online]. Available at: ncsc.gov.uk/ransomware/home [Accessed: 30 April 2026]
- [6] National Cyber Security Centre (NCSC). (2023). 10 Steps to Cyber Security. [Online]. Available at: ncsc.gov.uk/collection/10-steps [Accessed: 30 April 2026]
- [7] Verizon. (2024). Data Breach Investigations Report (DBIR). [Online]. Available at: verizon.com/business/resources/reports/dbir [Accessed: 30 April 2026]
- [8] OWASP Foundation. (2021). OWASP Top Ten. [Online]. Available at: owasp.org/www-project-top-ten [Accessed: 30 April 2026]

Appendix A: Board Presentation

The following slides were made as a 10-minute presentation to the Board of Directors at HPA with respect to the key findings and recommendations highlighted in this report. The presentation includes information related to the recent security breaches, threat environment, policy considerations, mitigation actions, monitoring and incident management procedures, employee education, and areas requiring approval from the board.





Data Security and Governance Framework

CONFIDENTIAL

Slide 1

What I'll Cover Today

A 10-minute board briefing on HPA's security framework

- 01** What went wrong at HPA recently
- 02** The threats we are facing
- 03** Security policies we need
- 04** Practical protective measures
- 05** Monitoring and incident response
- 06** Training the whole team
- 07** What I need the board to approve

Slide 2

What Has Gone Wrong at HPA

Two serious incidents that demand immediate action

Ransomware Attack

Attackers got into HPA's analytics servers and encrypted all files. Operations were disrupted and recovery took significant time and money.

Unauthorised Cloud Access

Patient data stored in the cloud was accessed by people who should not have had access — caused by a cloud storage misconfiguration.

Why this matters to the board:

UK GDPR Fines

Up to £17.5m or 4% of global turnover

NHS DSP Toolkit

Mandatory annual compliance — failing risks NHS contracts

Reputation

Hospitals trust HPA with sensitive patient data

Slide 3

The Threats HPA Is Facing

External attacks and internal risks — both must be addressed

FROM OUTSIDE

- Ransomware — locking files for ransom
- Phishing — tricking staff with fake emails
- Cloud misconfiguration — data left exposed
- Organised criminal groups (APTs)
- Attacks through third-party suppliers
- DDoS — crashing systems with fake traffic

FROM INSIDE

- Deliberate data theft by a staff member
- Staff mistakes — weak passwords, wrong BYOD use
- People with more access than they need
- Personal apps used to store work data (shadow IT)
- Unsecured physical access to servers

Framework lens: CIA Triad — Confidentiality | Integrity | Availability

Slide 4

Security Policies We Need

Aligned with ISO 27001 | NIST CSF | UK GDPR

Access Control

Only give people access to what they need. MFA on everything. Review every 3 months.

BYOD Policy

Personal devices must use approved security software. Remote wipe enabled. No tampered devices.

Password Policy

Minimum 14 characters. No reuse. Change every 90 days. Use a password manager.

Data Classification

Patient data = Restricted. Always encrypted when stored and when sent anywhere.

Incident Response

Report anything suspicious within 1 hour. Notify the ICO within 72 hours if patient data involved.

Acceptable Use

Company systems for work only. Activity is monitored. Breaking the rules = disciplinary action.

Slide 5

What We Need to Put in Place

Seven practical measures — colour coded by priority

Switch on MFA

Even if a password is stolen, attackers still cannot log in. Authenticator app on all systems.

DO NOW

EDR on Every Device

Watches for threats in real time. Stops ransomware before it can spread across the network.

DO NOW

Fix Cloud Security

CSPM tool finds misconfigurations automatically — catches issues before attackers do.

DO NOW

Zero Trust Network

No device trusted automatically. All access verified. Limits damage if someone gets in.

3 MONTHS

3-2-1 Backups

Three copies, one offline. Tested monthly. Best protection against ransomware recovery.

1 MONTH

Patch Fast

Critical updates within 48 hours. Weekly vulnerability scans across all systems.

ONGOING

Slide 6

Monitoring and Responding to Incidents

Ongoing detection + a clear 7-step plan when things go wrong

What to Monitor 24/7

- SIEM — one central security dashboard
- Failed logins and unusual access times
- Large data downloads or exports
- Changes to security settings or admin accounts
- Cloud activity — new resources, permissions

7-Step Response (NIST SP 800-61)

DETECT

TRIAGE — how serious?

CONTAIN — isolate & lock

NOTIFY ICO (72 hrs)

ERADICATE — remove threat

RECOVER — restore backups

REVIEW — learn from it

Slide 7

Training the Whole Team

Human error causes most breaches — training is just as important as technology

01 Annual Online Course

All staff, every year. Covers phishing, passwords, data handling, incident reporting. Completion tracked.

02 Monthly Fake Phishing

Simulated phishing emails to all staff. Click the link? Instant short training module. Results to board quarterly.

03 Role-Specific Training

IT admins: cloud & privileged access. Developers: OWASP Top 10 [8]. Finance/HR: email fraud.

04 New Starter Training

Security training before any system access. Sign the Acceptable Use Policy on day one.

05 Security Champions

One volunteer per team promotes good habits. Monthly newsletters + anonymous reporting channel.

NHS England (2023) [4]: Regular phishing simulations can cut staff click-through rates by up to 70% within 12 months.

Slide 8

What I'm Asking the Board to Approve

Standards this framework meets + priority actions needed now

Standards This Framework Meets

UK GDPR [1]	Patient data protection. 72-hr breach reporting.
NIST CSF [2]	Identify, Protect, Detect, Respond, Recover.
ISO 27001 [3]	International information security management.
NHS DSP Toolkit [4]	Annual compliance for NHS data processors.
NCSC 10 Steps [6]	UK government baseline cyber guidance.

Priority Actions for Approval

DO NOW	Deploy MFA across all systems
DO NOW	Install EDR on all staff devices
DO NOW	Implement CSPM for cloud environments
1 MONTH	Set up and test 3-2-1 backup system
3 MONTHS	Move network towards Zero Trust architecture
ONGOING	Annual training + monthly phishing tests

Slide 9

To Sum Up

2

Recent Incidents

Ransomware + Cloud breach

6

Policies Needed

Clear, written, enforced

7

Protective Measures

Technical + operational

5

Training Tracks

All staff covered

The Bottom Line

Both incidents were preventable. With the right controls in place, HPA can protect patient data, stay compliant with UK law, and keep the trust of the NHS organisations that rely on it. These measures are practical and achievable — they just need board commitment.

Thank you — happy to take any questions

Thomas Pereira | 2442400 | ACCA4024 | Amit Naik | 30 April 2026

Slide 10

The original PowerPoint file is also available at: [\[HPA Final Presentation.pptx\]](#)