Information Security Management & Governance

TABLE OF CONTENTS

INTRODUCTION

The NHS COVID-19 app has proven to be widely popular nationwide, with over 20 million downloads [34] processing gigabytes of data per second. This sensitive data, as well as NHS's quality assurance, is at stake. A comprehensive, legal security policy, backed by developers and management, is one safeguarding solution. In this age of information, applications should be secured on the software [3] and legal [35] level to ensure longevity and success.

To combat these concerns, this report will depict in technical detail:

⇒ Valuable business assets, how or why they should be secured and what can be done to minimise circumvention risk to regulations.

⇒ Inventory of practices and exercises that support the policy, how and why concerned parties must be compliant to them.

⇒ Factors and legislations considered during policy production, direction of the content in the awareness plan.

⇒ Promotional programmes raising awareness of current security concerns [10-11]. These programs would also portray how to ensure individuals permanently absorb key points within the policy quickly.

ASSET MANAGEMENT & RISK ANALYSIS

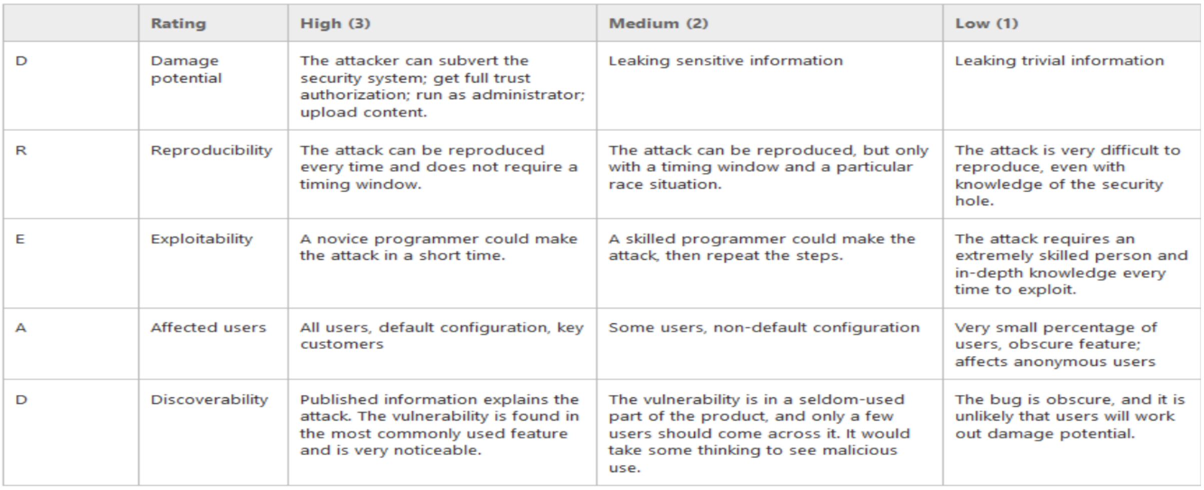
All organisations have an economic and legal interest in securing property they consider theirs. Mostly conducted for insurance and tracking reasons, it is also published to stakeholders and investors who require availability and usability knowledge of the app's assets [36]. There are automatic asset management solutions [37] that will prove useful in the short term before internal knowledge has increased to the point of independence.

Asset What to protect?	**Classification & Owner [40]** Classification conducted by an IAO* or SIRO* and approved by a SIRO or AO* (dependent on asset type) [38] under ISO 27001 [52]. Who is it important to?	**Value & Protection** Why are they valuable? How should they be protected?
Patient Databases Location data, test results, device details (for analytics).	✓ Informational Digital Asset. ✓ Could also be physical [39] if customer requested personal data and a letter was compiled. ✓ Certified as confidential under GDPR [8]. ✓ Important to patients, have the most to lose (their extremely private health information) if confidentiality is breached.	⇒ Database contains sensitive information with potential reputational risk [5]. ⇒ Access requests (human or otherwise) should be assessed and logged. ⇒ Data changelogs watched for abnormal behaviour [54], training of staff

		ensuring records are accurate. ⇒ Retention of redundant patient data evaluated regularly [53]. ⇒ Compulsory procedures developed to counter data exposure or corruption e.g. restoring from backup, preparing for reputational backlashes [56], signing off changes.
Application Software/Code Application itself, code and other software (i.e. Bluetooth).	✓ Software Digital Asset. ✓ Important to NHS to maintain positive software reputation (buggy or insecure COVID-19 app will see less use) and retail industry (stores rely on the app's track-and-trace check-in system [43]). ✓ Access to sensitive code is certified as restricted only to those who require it [45]. ✓ SIRO will oversee handling of risks to the codebase and application.	⇒ App is NHS property, can file lawsuits if utilised without permission [41]. Arbitrary app's utilising NHS brand are gaining prestige from popularity they did not forge themselves, drawing profit and data away from the NHS. ⇒ Code changes tracked and reviewed. Software tested prior to deployment in sandbox environments (or downtime periods if not possible) [55].
Servers Processes requests from application clients.	✓ Physical Digital Asset. Susceptible to damage or unauthorised USB interfacing that breaks CIA* [44]. ✓ Crucial to NHS to keep app operational (e.g. servicing results, track-and-trace) ✓ Server configuration changes can be breaking [46], access regarded as confidential (admins and authenticated clients exempted and responsible for access management). ✓ Regarding physical access, data centre security officers take ownership of	⇒ Defective servers equal excess strain on operational ones and inaccurate statistics for judging lockdown procedures. ⇒ Server logs and permission hierarchies track users. Similar system can be put in place for

	preventing physical attacks and certifying safety protocols are not flouted.	physical access to racks. ⇒ Ransomware attacks on the rise [57], policies enforcing constant threat updates and backup handling important in defending against this.
Secret Credentials Username/passwords or keys that allow application or developer authentication.	✓ Intangible information assets. Also labelled as service assets because they serve employee access to other tools. ✓ Developers require secret credentials otherwise valuable services will be unusable [47]. ✓ Individual entries assigned classifications (global, restricted, top-secret, etc) [48] by developers. Credentials bucket itself handled same as other assets.	⇒ Can provide root access. ⇒ Leaking of such credentials will reduce trust in handlers [58]. ⇒ Handlers trained in good credential storage and distribution practices and course of action on expiry or release. ⇒ Training provided to senior developers on classifying. It would be foolish to classify root server access SSH keys as “global”.
Copyrights/Licenses Legal rights to name, software and app contents that the NHS published.	✓ Another intangible asset, consisting of TOS Bluetooth development toolkits, penetration testing contracts, etc ✓ Valuable to NHS legal team. Tasked with identifying licencing documents if a term has been violated (as well as the course of action [50]). ✓ Most documents public knowledge but can be escalated to confidential. ✓ Developers responsible for honouring third party software TOS*. ✓ Legal team handles licensing of software assets.	⇒ Broken agreements result in financial, reputational and/or termination consequences [49]. ⇒ Document specifics and changelogs recorded, tracing tampering attempts. ⇒ Non-legal staff educated on legal repercussion protection. ⇒ Legal team should be familiar with distribution, basic functionality and software breach procedures.

Asset complexity varies depending on the laws, employee morality, intellectual property, and profit groups they fall under. As such, the application will encounter equally intriguing and layered risks utilising one of these valuables as an avenue. Risk analysis is imperative in identifying and countering these threats before they can occur [59]. Risk analysis will be conducted using the CRAMM tool (suitable for large, public sector organisations like the NHS) [60] but it likely could also have been conducted using Octave to benefit from its close-knit team ideology [61]. Stage 1 asset inventory (establishment of objectives) has been completed as well as Stage 3 (countermeasure recommendations) partially, so Stage 2 (threat ranking and types) will be the focus here. In tandem with CRAMM, STRIDE [65] is used for establishing the threats and DREAD for ranking the seriousness of them (as seen in figure 1).



	Rating	High (3)	Medium (2)	Low (1)
D	Damage potential	The attacker can subvert the security system; get full trust authorization; run as administrator; upload content.	Leaking sensitive information	Leaking trivial information
R	Reproducibility	The attack can be reproduced every time and does not require a timing window.	The attack can be reproduced, but only with a timing window and a particular race situation.	The attack is very difficult to reproduce, even with knowledge of the security hole.
E	Exploitability	A novice programmer could make the attack in a short time.	A skilled programmer could make the attack, then repeat the steps.	The attack requires an extremely skilled person and in-depth knowledge every time to exploit.
A	Affected users	All users, default configuration, key customers	Some users, non-default configuration	Very small percentage of users, obscure feature; affects anonymous users
D	Discoverability	Published information explains the attack. The vulnerability is found in the most commonly used feature and is very noticeable.	The vulnerability is in a seldom-used part of the product, and only a few users should come across it. It would take some thinking to see malicious use.	The bug is obscure, and it is unlikely that users will work out damage potential.

Figure 1:

DREAD risk rankings

J.Alhassan, E.Abba, O.Olaniyi, V.Waziri (2016)

http://ceur-ws.org/Vol-1830/Paper16.pdf

PATIENT DATA

The disclosure or tampering of data as sensitive as COVID-19 results would create serious repercussions against the NHS [1] as breaking patient confidentiality is a serious taboo in healthcare [63]. Therefore, a DREAD ranking of 12/15 (32232) would be suitable for test results, narrowly avoiding the rank 3 bracket by recent relaxation of patient confidentiality regulations [62]. Location data, averaging 11/15 (23222), is protected and enforced with financial and reputational consequences under GDPR [7-8].

Furthermore, corruption or access denial of the same data can be potentially more damaging [103]. Inefficiency is often claimed to be the killer of progress and, regarding denial of access to positive test results, the exponential progress would plummet. Unclean data can cost organisations millions in revenue [64] and is relatively easy to achieve with authorised database commands, hence the 14/15 (32333).

To counter unauthorised access (for both threats), CRUD requests should be evaluated and logged by IAA's*, with a compulsory verification procedure for new parties to pass before granted access [54]. Redundant or unused data must be deleted or archived away from active records after an extended period. Compartmentalisation is key when ensuring data privacy from unwanted advertisers, but it can also be true for cyber-attack prevention [66]. Finally, mandatory training should be assigned to database administrators on the safest methods of database interaction, as well as how to test new features safely.

APPLICATION SOFTWARE/CODE & SERVERS

Major frameworks have been subject to constant security aches [67-68] before and even Bluetooth is not safe from these attacks [3]. Therefore, learning from mistakes and keeping software and dependencies up to date is imperative for longevity [104]. If funding is available, bug bounty programs are helpful feedback tools to NHS developers for identifying security holes in both the app and its infrastructure.

However, each software implementation is different and contains variable factors. Adopting a TDD* framework [69] will help to identify bugs and vulnerabilities specific to the app prior to each release. Code that is tested should also be inspected prior to deployment, ideally by multiple developers providing constructive feedback. The endgame of attackers is to achieve escalation of privileges and subversion of security controls, both of which are breaking threats and deserving of a 11/15 (32132).

These changes will be a good starting point for reducing risk to the backend too, but safeguards must also be instigated on the servers that manage the app. A server not properly processing requests (for whatever reason) is a liability on the others, breeding grounds for DOS hazards [70]. If left unchecked, spiralling further down the chain can occur to coronavirus restriction planners, who are given inaccurate tracking data due to a lack of it available. Post-DOS, efficiency levels could be lost forever if the servers must be wiped and reinstalled from backup due to ransomware or deletion. As such, depending on the scale of an attack, the rank could be as high as 15/15!

All data handlers (and databases) should be backed up on a separate network to the source to prevent corruption of both sources. Then access (physical and digital) should be logged and evaluated in a similar manner to the patient databases, including different hierarchies granted separate levels of admission depending on how much is needed for the job purpose. Servers can be accessed via USB so these physical controls are necessary.

CREDENTIALS AND COPYRIGHTS

In general, DREAD classification of credentials is difficult as it is dependent on the individual level of access. Generally it will be high band (10-15) as these are secret for a reason and require revocation on exposure. During storage, they need to be kept inside encrypted or locked locations (locked cabinets if the credential is a physical key or staff card). Access groups (multiple user accounts grouped under one credential access policy) can help with distributing credentials to multiple users at once and will also be useful for tracking and modifying who has access.

Like credentials, copyright/license agreements vary in accessibility and complexity, but will also have a process of appeal for information under certain conditions (usually for court cases and legal concerns). Restricted licences will mostly consist of agreements that would detrimental if made public (e.g. penetration testing contracts). The risks of a Bluetooth contract becoming public are relatively low at 7/15 (21121) but could be financially damaging if the NHS have broken terms. A higher potential risk, 12/15 (22323), would be present if a penetration testing contract became employee knowledge, as the forewarned results of the testing will not accurate.

As expanded upon later, non-legal staff should be educated on protecting themselves and the NHS from legal repercussions. To ensure the legal team is equally informed on the development side, they should be familiar with the distribution, basic functionality and breach procedures the developers will be constructing and following. Both measures will see increases in employee co-operation and a forward-thinking workforce.

LAWS & REGULATIONS

Achieving compliance with relevant regulations and standards will be a staple goal of the policy, showing the NHS is security aware and complying with data protection standards. One of those standards is the Data Protection Act 2018 (GDPR), its clauses and articles enforcing standards against asset patient data. The Data Protection Act 1998 was repealed by the 2018 version [17] (although that may change with Brexit and the policy adjusted accordingly when that occurs), so it will not be discussed.

Quoting articles 4(13-15) and 9 of GDPR [9], COVID-19 test result health data is classed as sensitive [72] and forbidden from processing [71] (although recent regulations [73] have permitted sharing of test results if members of the public are at risk from infection [29]). The issue here is the under or over processing of a positive test result accounting for article 6 [74]. Process too much and the app will break confidentiality in the law's view but processing too little will result in a loss of trust and effectiveness in the app that cannot even warn others of a possible infection (the entire purpose of it!). The Health and Social Care Act 2001 [21] and Health Service (Control of Patient Information) Regulations 2002 [22] will be used to define exactly when it is legal to disclose confidential coronavirus results information [Section 1.2.a of 22].

In addition to this, recital 39 of GDPR [75] concerns right of user data erasure after a set period if it becomes redundant or permission is withdrawn. The danger is the holding of said data for an unnecessarily extended period, a similar situation that Facebook was snagged by [76] (fined £500,000 [77] and could have suffered further [29]). With this penalty looming, its imperative data is not placed into storage or backup and "forgotten" by automation processes. If that backup is breached or the data makes its way back into the system, recital 39 is broken.

The Computer Misuse Act 1990 [16] defines the threat and crime to the functionality of the app, especially sections 1 and 3. The NHS has been aggressively digitalising their records over the past 5 years [78] which generally equals more employee's and terminals helping to manage the increased influx of information. What is of concern is the threat of malicious inside actors seeking to damage software assets or steal data through these terminals behind the NHS firewall. Furthermore, malware could be installed on app servers to influence traffic to an attacker's discretion [79]. If the security policy is to be compliant, management will have the power to remove and arrest these insiders before they can do further damage. On the other hand, ensuring the policy is implemented effectively will result in less technical members of staff struggling to maintain a constant state of alert [80]. Care and attention will need to be used in devising the awareness plan to ensure it is suitable and easily absorbed.

Finally, since this is a health service app, regulations enforcing medical standards will be cited in the policy. The NHS Confidential Code of Practice 2003 [18] , while technically only bound to the NHS, is as good as law for staff members. Staff members who tamper with the app's data can be dismissed by defying this code and subsequently arrested under GDPR [20]. By protecting patient data assets with tracking and securement systems (e.g. limited signed authorisation, defensive programming, bug tracking and bounty systems, etc [81]), the NHS is protected from lawsuits claiming GDPR, code of practice or computer misuse act violations. However, it is easy for Annex A2 [18] to be mishandled, even by medical professionals [82], so the app must be open with how data is handled and exactly what it possesses.

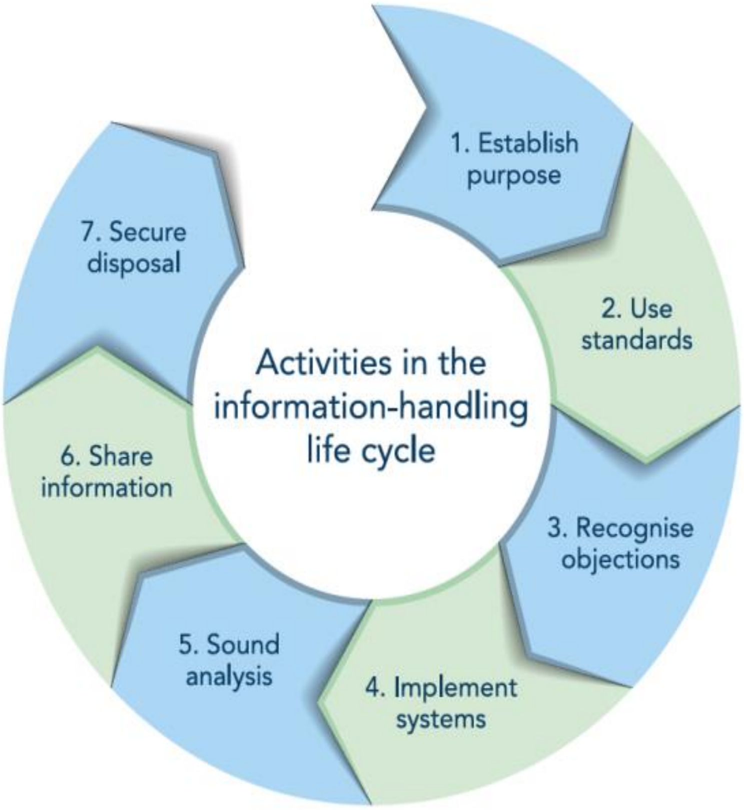


Figure 2 - Activities in the information handling cycle [84].

This represents how patient data is evaluated and processed (if at all).

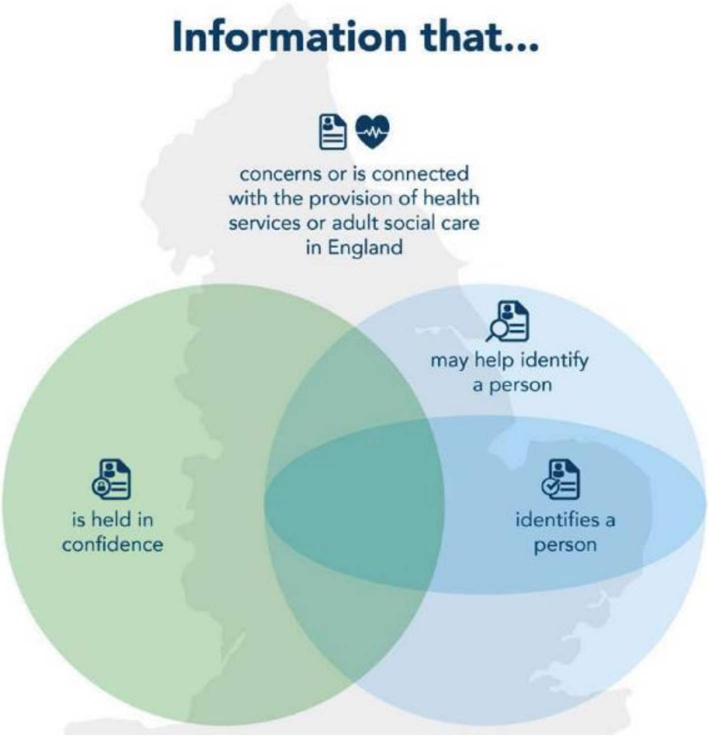

Information that...
concerns or is connected with the provision of health services or adult social care in England
may help identify a person
is held in confidence
identifies a person

Figure 3 - Definition of confidential information in scope for the code of practice on confidential information [84].

This represents who patient information can be distributed to and when.

SECURITY POLICY

1) Accountable Officer (AO)

a. *Tasked with…*

i. Reviewing/adjusting this document annually to reinforce standards from the highest executive level downwards. It is their job to verify that this policy will pass the ISO 27001 certification {19}.

ii. Providing risk assurance reports to the board based on feedback from SIRO's and investigations.

iii. Ensuring laws/regulations and standards are complied to across the NHS.

iv. Promoting NHS security practices and policies with the awareness plan.

b. *Should be…*

i. Resourceful at obtaining obscured information from technical sources and communicating it to non-technical employees

ii. Able to accurately scope out investigations into systems prior to being employed and experienced in executive activities (preferably in the health sector).

iii. Able to understand and parse the ISO series [85] of standards, especially 27001 as that will be what this policy is certified against.

iv. Aware of CISO's* position and can work with them to implement solutions and training programs.

2) Responsibilities

a. All staff will maintain security professionalism and should be aware of what is expected of them to protect the NHS. They will also complete assigned security training on time and without rush.

b. Staff should not attempt to elevate their access privileges beyond their assigned level and without a due audit determining whether an elevation of rights is justified.

c. Staff will not divulge, copy, release, sell, loan, alter or destroy NHS or application information without a valid business purpose and/or authorization [83].

d. Only the bare minimum of data should be collected from a patient for the app to function effectively. Redundant data not to be held longer than 6 months and the owner should be reminded of the approaching deletion and their options.

e. Protect CIA of application, server, patient and staff assets according to each asset's classification and recommended safeguarding practices.

f. Server rooms and data centres must meet modern health, safety and security standards [91-92] to prevent physical breaches and financially damaging events (i.e. power surges, fires, etc).

g. Report suspicious activity (no matter where or how doubtful) to the information security or asset team (include contact details in final policy).

3) Resources

a. *Bluetooth*

i. Developers to ensure the application and code are compliant to Bluetooth's fair use policies [88].

ii. Bluetooth location data disassociated with device information to prevent accidental tracking and must be as truthful/unaltered as possible.

iii. SIRO's should keep updated of existing vulnerabilities and ensure risk analysis is conducted monthly to keep up to date (whether there has been a new vulnerability reported or not).

b. *Hosting Services (e.g. domain registrars, server rental boards, cloud platforms, etc)*

i. The application must conform to provider end user licence agreements and other legislations governing how they allow their service to be used (verified by an IAO risk analysis on procurement of said service).

ii. New service proposals ought to be appraised by a SIRO and AO, checking the service's quality assurance track record and security culture. They must also reason what asset data classifications are safe to be stored on the service based on a risk assessment of the service and data combined [89].

4) Users

a. New development and admin users must undergo an application process which the security team will evaluate for business needs and trust in the employee [27].Once approved, employees shall not abuse their access and/or elevate unauthorised actor privileges.

b. User accounts should be secured with modern and multilevel techniques [90] with these measures reviewed monthly.

c. New patients will be informed on the data collection process along with how to opt out or request what data the app possesses.

d. Employees (technical or not) will have their user accounts deleted on exit of the company or if they no longer require the account to achieve their job goal. Patients may request to have their location data and results data deleted if it does not put members of the public at risk.

AWARENESS PLAN

In-house testing and training programs compulsorily issued to staff to educate them on policy standards and aims. All staff utilising the app's services are on the frontline representing the business and protecting the assets, opening a major, human-error security hole if not trained appropriately [31]. Furthermore, failing to show sufficient evidence of training programs can leave the NHS open to legal action against ISO27002 7.2 [94] and GDPR Article 60:1 [95]. If set-up or distribution proves to be an issue initially, there are companies [101] who offer help with installing solutions and delivering content (e.g. Barracuda PhishLine [102] is a quick launch, simulated phishing attack tool that the NHS could deploy against database administrators to test awareness). However, in the long-term, this would likely prove to be redundant as opposed to us maintaining such a system ourselves.

Awareness training should be engaging and enjoyable, encouraging a higher intake of information and stronger desire to complete programs in the future [93]. Games, social/group activities, rewards (trips, time off, etc) can incentivise completing training so long as it is applied sparingly to avoid employee's rushing [4] it or abusing the rewards system [96]. These activities must also be relatable to the employee's, fostering professionalism in data handling or identifying coronavirus fake news.

Training will be issued to any user that has access to the app's systems or patient databases, technically experienced or not [97]. General security practices (strong passwords, being suspicious of email attachments, etc) will be the focus but will also include security team points of contact and current, likely threats (based off the DREAD rankings above) that the employee group will encounter. This is the key part. While there will be training programmes for all staff, there will be additional training for staff that is based on their business sector (development, data collection and management, application finances, etc). Compartmentalizing guidance to only staff that will need it will slash training time, boredom and risk of information overload [98]. To further reduce repetitive information burnout, small sessions will be staggered every 6 months in lieu of an in all in one go methodology [32-33].

Complementing in-house training will be practical events seeking to appeal to hands-on learners. Practical activities could even include games amongst the infrastructure staff for who can steal other staff cards [100]! It could also be possible to authorise an organisation wide simulated phishing campaign [99] against app employees (posing as management or a doctor with queries about the app's capabilities). Both techniques provide instant feedback on the effectiveness of in-house training as well as an excellent guidance tool for IAO's deciding where to dedicate their learning resources.

Finally, it is critical to keep the awareness plans as fresh and up-to-date as possible after each business year. Usually the AO or SIRO's will catch most flaws but there will be a feedback questionnaire option open for employees to submit their own ideas and activities at the end of each session. No-one would enjoy completing the same, plain assignment each time it was required so varying how staff learn these concepts will be crucial to ensure a strong sense of security awareness is maintained.

CONCLUSION

To conclude, an app without a visible log in system contains a surprising number of avenues into patient data scraping by means of hijacking assets and employee accounts. As such, the security policy has been similarly skewed towards protecting patients more so than the NHS (especially with multiple legislations requiring satisfaction in this area). That does not exclude raising awareness of other vulnerabilities however as they can prove just as effective in crippling company operations. Looking at the potential consequences (legal, financial and reputation) of a security breach, the NHS should approve the hiring of an asset owner and assurance team on the basis that the cost of doing so would be inferior to the breach itself.

REFERENCES & APPENDIX

REFERENCES

1. Information Commissioner's Office (2019). *London pharmacy fined after "careless" storage of patient data* [Online]. Available at https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/12/london-pharmacy-fined-after-careless-storage-of-patient-data (Accessed 9/11/2020).
2. Cyber news group (2020). *How Is The NHS Covid-19 App Cyber-Secure?* [Online]. Available at https://www.cybernewsgroup.co.uk/how-is-the-nhs-covid-19-app-cyber-secure (Accessed 9/11/2020).
3. Insinuator (2020). *Critical Bluetooth Vulnerability in Android (CVE-2020-0022) – BlueFrag* [Online]. Available at https://insinuator.net/2020/02/critical-bluetooth-vulnerability-in-android-cve-2020-0022 (Accessed 9/11/2020).
4. ZDNet (2018). *Rushed privacy features result in sloppy security* [Online]. Available at https://www.zdnet.com/article/rushed-privacy-features-result-in-sloppy-security (Accessed 9/11/2020).
5. Ellen Neveux (2020). *Reputation Risks: How Cyberattacks Affect Consumer Perception* [Online]. Available at https://www.securelink.com/blog/reputation-risks-how-cyberattacks-affect-consumer-perception (Accessed 10/11/2020).
6. Indrajeet Deshpande (2020). *What Is Customer Data? Definition, Types, Collection, Validation and Analysis* [Online]. Available at https://www.toolbox.com/marketing/customer-data/articles/what-is-customer-data/#_002 (Accessed 10/11/2020).
7. European Commission (2016). *What personal data is considered sensitive?* [Online]. Available at https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_en (Accessed 10/11/2020).
8. Which (2018). *What counts as personal data?* [Online]. Available at https://www.which.co.uk/consumer-rights/advice/what-counts-as-personal-data-according-to-gdpr (Accessed 10/11/2020)
9. Which (2018). *Data Protection Act 2018 (GDPR)* [Online]. Available at https://www.which.co.uk/consumer-rights/regulation/gdpr-data-protection-act#collecting-your-personal-data (Accessed 10/11/2020)

10. Bojana Dobran. *RSA SecurID Cybersecurity Attack* [Online]. Available at https://phoenixnap.com/blog/famous-social-engineering-attacks (Accessed 10/11/2020)

11. Eric Chabrow (2011). *'Tricked' RSA Worker Opened Backdoor to APT Attack* [Online]. Available at https://www.bankinfosecurity.com/tricked-rsa-worker-opened-backdoor-to-apt-attack-a-3504 (Accessed 10/11/2020)

12. UK Government (2020). *NHS COVID-19 app: privacy notice* [Online]. Available at https://www.gov.uk/government/publications/nhs-covid-19-app-privacy-information/nhs-test-and-trace-app-early-adopter-trial-august-2020-privacy-notice (Accessed 10/11/2020)

13. Nate Lord (2020). *What is a Data Protection Officer (DPO)? Learn About the New Role Required for GDPR Compliance in 2019* [Online]. Available at https://digitalguardian.com/blog/what-data-protection-officer-dpo-learn-about-new-role-required-gdpr-compliance (Accessed 10/11/2020)

14. Information Commissioner’s Office (2020). *Data protection officers* [Online]. Available at https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-officers (Accessed 10/11/2020)

15. Packet Labs (2020). *What is Data Classification?* [Online]. Available at https://www.packetlabs.net/data-classification/#:~:text=Data%20Classification%20in%20Government%20organizations,%2C%20Confidential%2C%20Internal%2C%20Public (Accessed 11/11/2020)

16. UK Government (1990-2020). *Computer Misuse Act 1990* [Online]. Available at https://www.legislation.gov.uk/ukpga/1990/18/contents (Accessed 11/11/2020)

17. UK Government (1998-2018). *Data Protection Act 1998* [Online]. Available at https://www.legislation.gov.uk/ukpga/1998/29/contents (Accessed 11/11/2020)

18. DH/IPU/Patient Confidentiality (2003). *NHS Confidentiality Code of Practice* [Online]. Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/200146/Confidentiality_-_NHS_Code_of_Practice.pdf (Accessed 11/11/2020)

19. UK Government (1998-2020). *Human Rights Act 1998* [Online]. Available at https://www.legislation.gov.uk/ukpga/1998/42/contents (Accessed 11/11/2020)

20. Corporate Information Governance (2019). *Confidentiality Policy* [Online]. Section 3.9 only. Available at https://england.nhs.uk/wp-content/uploads/2019/10/confidentiality-policy-v5.1.pdf (Accessed 11/11/2020)

21. UK Government (2001-2020). *Health and Social Care Act 2001* [Online]. Available at https://www.legislation.gov.uk/ukpga/2001/15/contents (Accessed 11/11/2020)

22. UK Government (2002-2020). *The Health Service (Control of Patient Information) Regulations 2002* [Online]. Available at https://www.legislation.gov.uk/uksi/2002/1438/contents/made (Accessed 11/11/2020)

23. Davey Winder (2018). *Social engineering: The biggest security risk to your business* [Online]. Available at https://www.itpro.co.uk/social-engineering/30017/social-engineering-the-biggest-security-risk-to-your-business (Accessed 11/11/2020)

24. Ray Dunham (2020). *Information Security Policies: Why They Are Important To Your Organization* [Online]. Available at https://linfordco.com/blog/information-security-policies (Accessed 12/11/2020)

25. Thomson Reuters (2020). *Computer Fraud and Abuse Act (CFAA)* [Online]. Available at https://uk.practicallaw.thomsonreuters.com/2-508-3428?transitionType=Default&contextData=(sc.Default) (Accessed 12/11/2020)

26. Michael Gegick, Sean Barnum (2013). *Least Privilege* [Online]. Available at https://us-cert.cisa.gov/bsi/articles/knowledge/principles/least-privilege (Accessed 12/11/2020)

27. Kaspersky (2020). *The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within* [Online]. Available at https://www.kaspersky.com/blog/the-human-factor-in-it-security (Accessed 12/11/2020)

28. It Governance (2018). *GDPR penalties and fines* [Online]. Available at https://www.itgovernance.co.uk/dpa-and-gdpr-penalties (Accessed 12/11/2020)

29. NHS (2020). *Answer questions about your main symptom* [Online]. Available at https://111.nhs.uk (Accessed 12/11/2020)

30. IT Governance (2020). *Cyber security awareness training for employees* [Online]. Available at https://www.itgovernance.co.uk/staff-awareness (Accessed 13/11/2020)

31. Trustwave (2020). *Establishing a security awareness program* [Online]. Available at https://help.securitycolony.com/help/i-want-to-set-up-a-security-awareness-program-where-do-i-start (Accessed 13/11/2020)

32. Scott Ikeda (2020). *Phishing Awareness Training is Far From Permanent; New Study Shows the Effects Last Only a Few Months* [Online]. Paragraph 3. Available at https://www.cpomagazine.com/cyber-security/phishing-awareness-training-is-far-from-permanent-new-study-shows-the-effects-last-only-a-few-months (Accessed 13/11/2020)

33. Department of Health and Social Care (2020). *NHS COVID-19* [Online]. Available at https://play.google.com/store/apps/details?id=uk.nhs.covid19.production (Accessed 13/11/2020)

34. UK Government (2020). *NHS Test and Trace reaches record number of people as demand increases significantly* [Online]. Available at https://www.gov.uk/government/news/nhs-test-and-trace-reaches-record-number-of-people-as-demand-increases-significantly (Accessed 6/1/2021)

35. Bryan Seely (2021). Section *As somebody who has hacked into the US Secret Service, although you did it just to show them that it was possible to highlight a security flaw. What could be some of the possible reasons here? We're hearing that it was a software update, but is there any other things besides that that could be leading to the possibility that hackers can get in?* Available at https://www.euronews.com/2021/01/06/russia-likely-behind-huge-hack-on-us-government-say-security-services (Accessed 6/1/2021)

36. Corporate Finance Institute (2021). *What is Asset Management?* [Online]. Available at https://corporatefinanceinstitute.com/resources/knowledge/finance/asset-management/#:~:text=Asset%20management%20is%20the%20process,of%20individuals%20or%20other%20entities (Accessed 8/1/2021)

37. Kissflow (2019). *Everything You Need to Know Before Buying Asset Management Software* [Online]. Available at https://kissflow.com/finance/asset-management/asset-management-software-features/ (Accessed 8/1/2021)
38. NHS (2021). *GUIDANCE FOR INFORMATION ASSET OWNERS AND INFORMATION ASSET ADMINISTRATORS* [Online]. Available at https://www.sfh-tr.nhs.uk/media/1970/information-asset-owners-and-information-asset-administrators-guidance-version-5.pdf (Accessed 8/1/2021).
39. NHS (2020). *How to make a subject access request* [Online]. Available at https://digital.nhs.uk/about-nhs-digital/corporate-information-and-documents/publication-scheme/how-to-make-a-subject-access-request (Accessed 8/1/2021)
40. Luke Irwin (2019). *What is information classification and how is it relevant to ISO 27001?* [Online]. Available at https://www.itgovernance.co.uk/blog/what-is-information-classification-and-how-is-it-relevant-to-iso-27001 (Accessed 8/1/2021)
41. David Burkett (2016). *Software Licensing: Why It's Important and How It Can Help You* [Online]. Section *Why Software Licensing Is Important*. Available at https://workingmouse.com.au/innovation/software-licensing-why-its-important-and-how-it-can-help-you (Accessed 9/1/2021)
42. Free Software Foundation Inc (2007). *GNU General Public License Version 3* [Online]. Available at https://www.gnu.org/licenses/gpl-3.0.en.html (Accessed 9/1/2021)
43. Department of Health and Social Care (2020). *NHS COVID-19 app has been downloaded over 10 million times* [Online]. Available at https://www.gov.uk/government/news/nhs-covid-19-app-has-been-downloaded-over-10-million-times (Accessed 9/1/2021)
44. Debbie Walkowski (2019). *What is the CIA Triad?* [Online]. Available at https://www.f5.com/labs/articles/education/what-is-the-cia-triad (Accessed 9/1/2021)
45. Nate Lord (2020). *Principle of Least Privilege: A Best Practice for Information Security and Compliance* [Online]. Available at https://digitalguardian.com/blog/what-principle-least-privilege-polp-best-practice-information-security-and-compliance (Accessed 9/1/2021)
46. Asana (2021). *Communicating about breaking changes* [Online]. Available at https://developers.asana.com/docs/communicating-about-breaking-changes (Accessed 9/1/2021)
47. Andy Greenberg (2019). *Hackers Are Passing Around a Megaleak of 2.2 Billion Records* [Online]. Available at https://www.wired.com/story/collection-leak-usernames-passwords-billions (Accessed 9/1/2021)
48. Solarwindsmsp (2021). *Permission Level Guide* [Online]. Available at https://documentation.solarwindsmsp.com/passportal/documentation/Content/man-user-access/perm-level-guide.htm (Accessed 9/1/2021)
49. Robert Purchese (2017). *The Star Citizen makers are being sued by Crytek* [Online]. Available at https://www.eurogamer.net/articles/2017-12-14-the-star-citizen-makers-are-being-sued-by-crytek (Accessed 10/1/2021)
50. NHS (2012). *INTELLECTUAL PROPERTY RIGHTS: DEALING WITH INFRINGEMENTS* [Online]. Available at http://knowledge.nic.nhs.uk/documentDetails.aspx?docId=16 (Accessed 10/1/2021)

51. TermsFeed (2020). *5 Reasons Why You Need Terms and Conditions* [Online]. Available at https://www.termsfeed.com/blog/5-reasons-need-terms-conditions (Accessed 10/1/2021)
52. Sobhi Mahmoud, Andreas Wolf, Charles-Pierre Bazin de Caix, Bastien Gavoille (2013). *ISO/IEC 27001:2013* [Online E-Book]. Available at https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en (Accessed 10/1/2021)
53. Bryan Dunne (2018). *How long should you retain your employee data under GDPR?* [Online]. Available at https://www.siliconrepublic.com/enterprise/gdpr-data-retention#:~:text=GDPR%20does%20not%20specify%20retention,for%20which%20it%20was%20processed (Accessed 10/1/2021)
54. British Medical Association (2018). *Access to health records: Updated to reflect the General Data Protection Regulation and Data Protection Act 2018* [Online]. Available at https://www.bma.org.uk/media/2821/bma-access-to-health-records-june-20.pdf (Accessed 10/1/2021)
55. Lonnie Finkel (2017). *How to Protect Your Company's Software Assets Through Contract Protection* [Online]. Available at https://finkellawgroup.com/2017/12/07/protect-companys-software-assets-contract-protection (Accessed 10/1/2021)
56. Consolidated Technologies Inc (2018). *10 Common Causes of Data Loss* [Online]. Available at https://consoltech.com/blog/10-common-causes-of-data-loss (Accessed 10/1/2021)
57. Danny Palmer (2020). *Ransomware: Huge rise in attacks this year as cyber criminals hunt bigger pay days* [Online]. Available at https://www.zdnet.com/article/ransomware-huge-rise-in-attacks-this-year-as-cyber-criminals-hunt-bigger-pay-days (Accessed 10/1/2021)
58. Peninsula Team (2011). *Breach of Confidentiality at work* [Online]. Available at https://www.peninsulagrouplimited.com/topic/data-protection/employees-leak-confidential-information (Accessed 10/1/2021)
59. Terje Aven (2015). *Risk Analysis* [Online E-Book]. Available at https://books.google.co.uk/books?hl=en&lr=&id=41V_BwAAQBAJ&oi=fnd&pg=PR9&dq=risk+analysis&ots=okFrGG0Vxo&sig=1-mDedLRbO5_mVBeMKfDQ_slZAA&redir_esc=y#v=onepage&q=risk%20analysis&f=false (Accessed 11/1/2021)
60. Zeki Yazar (2002). *A qualitative risk analysis and management tool – CRAMM* [Online E-Book]. Available at http://130.18.86.27/faculty/warkentin/SecurityPapers/Robert/Others/Yazar2002_SANS_QualitativeRiskTool.pdf (Accessed 11/1/2021)
61. University Of Kansas (2019). *OCTAVE METHOD OF SECURITY ASSESSMENT* [Online]. Available at https://technology.ku.edu/octave-method-security-assessment (Accessed 11/1/2021)
62. Clare Dyer (2020). *Covid-19: Rules on sharing confidential patient information are relaxed in England* [Online]. Available at https://www.bmj.com/content/369/bmj.m1378 (Accessed 11/1/2021)
63. Ministry of Ethics (2014). *CONSEQUENCES OF BREACHING CONFIDENTIALITY* [Online]. Available at https://ministryofethics.co.uk/index.php?p=6&q=7 (Accessed 11/1/2021)

64. Matt Gibson (2020). *Dirty Patient Data Can Have Severe Consequences for Healthcare Providers* [Online]. Available at https://www.rightpatient.com/blog/dirty-patient-data-severe-consequences-healthcare-providers (Accessed 11/1/2021)

65. Rabani (2020). *WHAT IS STRIDE METHODOLOGY IN THREAT MODELING?* [Online]. Available at https://blog.eccouncil.org/what-is-stride-methodology-in-threat-modeling (Accessed 11/1/2021)

66. Paul Warwick (2019). *Why "Compartmentalisation" is the key to protecting your online privacy* [Online]. Available at https://medium.com/@privacyhivesoftware/why-compartmentalisation-is-the-key-to-protecting-your-online-privacy-b91d86482cd (Accessed 11/1/2021)

67. John Leyden (2020). *Latest web hacking tools – Q4 2020* [Online]. Available at https://portswigger.net/daily-swig/latest-web-hacking-tools-q4-2020 (Accessed 13/1/2021)

68. Jacob Kastrenakes (2015). *Adobe is telling people to stop using Flash* [Online]. Available at https://www.theverge.com/2015/12/1/9827778/stop-using-flash (Accessed 13/1/2021)

69. Agile Alliance (2002). *TDD* [Online]. Available at https://www.agilealliance.org/glossary/tdd/#q=~(infinite~false~filters~(postType~(~'page~'post~'aa_book~'aa_event_session~'aa_experience_report~'aa_glossary~'aa_research_paper~'aa_video)~tags~(~'tdd))~searchTerm~'~sort~false~sortDirection~'asc~page~1) (Accessed 13/1/2021)

70. BBC (2020). *Netflix to cut streaming quality in Europe for 30 days* [Online]. Available at https://www.bbc.co.uk/news/technology-51968302 (Accessed 13/1/2021)

71. OWASP (2021). *Credential Stuffing* [Online]. Available at https://owasp.org/www-community/attacks/Credential_stuffing (Accessed 13/1/2021)

72. Intersoft Consulting (2018). *Article 4: GDPR* [Online]. Available at https://gdpr-info.eu/art-4-gdpr/ (Accessed 14/1/2021)

73. Intersoft Consulting (2018). *Recital 51: GDPR* [Online]. Available at https://gdpr-info.eu/recitals/no-51/ (Accessed 14/1/2021)

74. The Aspiring Medics (2020). *Breaking Confidentiality* [Online]. Available at https://www.theaspiringmedics.co.uk/post/medical-ethics-breaking-confidentiality (Accessed 14/1/2021)

75. Intersoft Consulting (2018). *Article 6: GDPR* [Online]. Available at https://gdpr-info.eu/art-6-gdpr/ (Accessed 14/1/2021)

76. Intersoft Consulting (2018). *Recital 39: GDPR* [Online]. Available at https://gdpr-info.eu/recitals/no-39/ (Accessed 14/1/2021)

77. Elizabeth Denham (2018). *Supervisory Powers of the Information Commissioner: Monetary Penalty Notice* [Online]. Available at https://ico.org.uk/media/action-weve-taken/mpns/2260051/r-facebook-mpn-20181024.pdf (Accessed 14/1/2021)

78. Paolo Zialcita (2019). *Facebook Pays $643,000 Fine For Role In Cambridge Analytica Scandal* [Online]. Available at https://text.npr.org/774749376 (Accessed 14/1/2021)

79. NHS (2015). *Clinicians told to embrace digital technology* [Online]. Available at https://www.england.nhs.uk/2015/12/embrace-digital-tech/ (Accessed 15/1/2021)

80. Cisecurity (2021). *Insider Threats: In the Healthcare Sector* [Online]. Available at https://www.cisecurity.org/blog/insider-threats-in-the-healthcare-sector/ (Accessed 15/1/2021)

81. Carole Donaldson (2019). *4 Tips to Train Non-Technical Employees on Cybersecurity Awareness* [Online]. Available at https://thetrainingassociates.com/blog/train-non-technical-employees-cybersecurity-awareness/ (Accessed 15/1/2021)
82. Ian Levy, Stuart H (2020). *NHS Test and Trace app security redux* [Online]. Available at https://www.ncsc.gov.uk/blog-post/nhs-test-and-trace-app-security-redux (Accessed 15/1/2021)
83. Ian Leonard (2021). *Leading Oncologist 'Lost Confidence of Staff'* [Online]. Available at https://www.medscape.com/viewarticle/944170 (Accessed 15/1/2021)
84. It Governance (2021). *ISO 27000 Series of Standards* [Online]. Available at https://www.itgovernance.co.uk/iso27000-family (Accessed 16/1/2021)
85. Graeme Messina (2019). *Senior/Advanced Security Auditor Questions* [Online]. Available at https://resources.infosecinstitute.com/topic/top-30-security-auditor-interview-questions-and-answers-for-2019/ (Accessed 16/1/2021)
86. Health and Social Care Information Centre (2014). *Activities in the Information Handling Cycle* [Online]. Available at https://www.mansfieldandashfieldccg.nhs.uk/media/1953/confidential-information-code-of-practice-hscic-version-1.pdf (Accessed 16/1/2021)
87. Princeton university (2015). *Responsibilities* [Online]. Available at https://oit.princeton.edu/policies/information-security (Accessed 16/1/2021)
88. Bluetooth (2019). *Policies and Rules* [Online]. Available at https://www.bluetooth.com/about-us/governing-documents/ (Accessed 16/1/2021)
89. Anthony Caruana (2011). *Five questions to ask when choosing a cloud service* [Online]. Available at https://www.computerweekly.com/feature/Five-questions-to-ask-when-choosing-a-cloud-service (Accessed 16/1/2021)
90. Ian Maddox (2018). *12 best practices for user account, authentication, and password management* [Online]. Available at https://cloud.google.com/blog/products/gcp/12-best-practices-for-user-account (Accessed 16/1/2021)
91. Server Room Environments (2020). *Server Room Audits and Data Centre Design Standards* [Online]. Available at https://www.serverroomenvironments.co.uk/blog/data-centre-design-standards (Accessed 16/1/2021)
92. Tuvit (2021). *Data center certification according to EN 50600* [Online]. Available at https://www.tuvit.de/en/services/data-centers-colocation-cloud-infrastructures/din-en-50600/ (Accessed 16/1/2021)
93. The Defence Works (2020). *How to Make a Security Awareness Training Programme Fun* [Online]. Available at https://thedefenceworks.com/blog/how-to-make-a-security-awareness-training-programme-fun/#:~:text=Fun%20brings%20learning%20to%20life,building%20more%20effective%20training%20programs (Accessed 17/1/2021)
94. Secaware (2013). *ISO/IEC 27002:2013: 7.2 During employment* [Online]. Available at https://www.iso27001security.com/html/27002.html (Accessed 17/1/2021)
95. Intersoft Consulting (2018). *Article 70: GDPR* [Online]. Available at https://gdpr-info.eu/art-70-gdpr/ (Accessed 17/1/2021)
96. Lance Spitzner (2020). *How to Effectively Reward Secure Behaviors* [Online]. Available at https://www.sans.org/security-awareness-training/blog/how-effectively-reward-secure-behaviors (Accessed 17/1/2021)

97. NATASHA DEENEY (2020). *Why Is Security Awareness Training Important?* [Online]. Available at https://www.metacompliance.com/blog/why-is-security-awareness-training-important/ (Accessed 17/1/2021)
98. Lauren Zink (2017). *How to Tailor Security Awareness Training to Employees' Needs* [Online]. Available at https://www.securitymagazine.com/articles/88538-how-to-tailor-security-awareness-training-to-employees-needs (Accessed 17/1/2021)
99. CSSCloud (2021). *SIMULATED PHISHING CAMPAIGNS* [Online]. Available at https://www.csscloud.co.uk/simulated-phishing-campaigns/ (Accessed 17/1/2021)
100. admin@sparxoo.com (2020). *Cyber Security Top 10 Best Games To Make Your Employees Aware* [Online]. Available at https://www.livingsecurity.com/blog/10-best-games-cyber-security (Accessed 17/1/2021)
101. Steve Morgan (2020). *List Of Security Awareness Training Companies To Watch In 2020* [Online]. Available at https://cybersecurityventures.com/security-awareness-training-companies/ (Accessed 17/1/2021)
102. Barracuda (2021). *Barracuda PhishLine: Fight security threats with user awareness training.* [Online]. Available at https://www.barracuda.com/products/phishline (Accessed 17/1/2021)
103. Leo Kelion (2020). *Excel: Why using Microsoft's tool caused Covid-19 results to be lost* [Online]. Available at https://www.bbc.co.uk/news/technology-54423988 (Accessed 18/1/2021)
104. Acronis (2017). *The NHS cyber attack: What caused the attack?* [Online]. Available at https://www.acronis.com/en-gb/articles/nhs-cyber-attack/ (Accessed 18/1/2021)
105. Josh Fruhlinger (2019). *What is a CISO? Responsibilities and requirements for this vital leadership role* [Online]. Available at https://www.csoonline.com/article/3332026/what-is-a-ciso-responsibilities-and-requirements-for-this-vital-leadership-role.html (Accessed 18/1/2021)

APPENDIX 1 – ACRONYMS (IN ORDER OF APPEARANCE)

*IAO = Information Asset Owner – "members of staff who senior enough to make decisions on the asset" [38]

*SIRO = Senior Information Asset Owner – "SIRO provides briefings and reports to the Board on matters of performance and assurance". They also sign off decisions made by an IAO. [38]

*AO = Accountable Officer – "Chief Executive, has overall responsibility for ensuring information risks are assessed and mitigated to an acceptable level". SIRO's report directly to them [38]

*CIA = Confidentiality, integrity, availability – "Together, these three principles form the cornerstone of any organization's security infrastructure; in fact, they (should) function as goals and objectives for every security program" [44]

*TOS = Terms of Service – "A Terms of Service Agreement is a set of regulations which users must agree to follow in order to use a service" [51]

*IAA = Information Asset Administrator – "provide support to their IAO by ensuring that policies and procedures are followed". They handle the day-to-day maintenance of asset management [38].

*TDD = Test Driven Development – "a style of programming in which three activities are tightly interwoven: coding, testing (in the form of writing unit tests) and design (in the form of refactoring)." [69]

* CISO = Chief information security officer – “executive responsible for an organization's information and data security” [105].

APPENDIX 2 – NOTES

! When referring to “patients”, the report is referring to regular users of the app (not administrators, developers or medical staff)