NHS Digital

Data Security Standard 6

Responding to incidents

The bigger picture and how the standard fits in

2021/22

Information and technology for better health and care

Contents

Overview 3

Using professional judgment 4

Incident reporting system 5

Definition and scope 5
The incident reporting system 6
Incident management system 8
Investigation 8
Managing an incident 8
An informed and empowered audience 9
A Variety of Reporting routes 10
Notifying Local Leaders, National Bodies and individuals of a data breach 11
End point anti-virus 12
Anti-virus costs 12
Anti-virus coverage 12
Always on, always connected, always up to date 13
Blocking web malicious content 14
Application Management 14
Email server software 16
DMARC, DKIM and SPF 17
Spam, Spam everywhere but not a bite to eat 17
Acting upon known vulnerabilities 18
Which vulnerabilities? 18
Threats 18
Vulnerability 18
NHS Cyber Alerts Service 19
Repeat data security incidents 20
Monitoring 21
Fraud 22
Appendix 1 - 23
Table of Data Security Level 6 Assertions 23
Appendix 2 - 25
Useful resources 25
Appendix 3 – 27
The National Data Guardian Reports 27

Overview

The NDG's review Data Security Standard 6 states that:

"Cyber-attacks against services are identified and resisted and CareCERT security advice is responded to. Action is taken immediately following a data breach or a near miss, with a report made to senior management within 12 hours of detection."

"All staff are trained in how to report an incident, and appreciation is expressed when incidents are reported. Sitting on an incident, rather than reporting it promptly, faces harsh sanctions. The Board understands that it is ultimately accountable for the impact of security incidents, and bears the responsibility for making staff aware of their responsibilities to report upwards. Basic safeguards are in place to prevent users from unsafe internet use. Anti-virus, anti-spam filters and basic firewall protections are deployed to protect users from basic internet-borne threats."

Department of Health

Using professional judgment

The DSPT guidance (audit framework and associated “big picture guides”) is not exhaustive. They will not cover every eventually and professional judgement will be required in how the standard is met and audited.

Both sets of guidance endeavour to be vendor agnostic. You may have an excellent vendor-supplied system which is not referred to in the guides. That is not to discount such a system, which should be implemented and audited on its merits.

The required standards have to be achievable to those whose digital maturity is still “developing”. As a consequence, some of the measures outlined could be seen as quite manual. This does not mean that more sophisticated measures cannot be implemented.

At times the big picture guides may go further than the audit guides and vice versa. Only the most binary of assertions would lead to one answer. The divergence of guides is either following an implementation theme to the end or the next logical audit artifact

When implementing or auditing please have regard to the intent of the evidence, assertions, standards and ultimately the whole 10 data security standards themselves. It is not the intention of the DSPT to create tick lists of items to be implemented and audited that bear little resemblance to actual practice.

Incident reporting system

Definition and scope

An incident can have many definitions ranging from an IT service desk type definition to a wider business continuity incident.

NB. For the purposes of the Data Security and Protection toolkit an incident is considered to be an event that has a data security implication (Confidentiality, Integrity or Availability). If the incident also involves personal confidential information, it can also be a data breach which requires reviewing to see if it is notifiable to interested parties, including the ICO.

Incident reporting is a method or means of declaring any unusual problem, occurrence or other situation that may comprise (or is likely to lead to) undesirable effects, or that is not in accordance with established policies, procedures or practices:

- disclosure or loss / theft of information
- inappropriate access and / or modification
- cyber-attacks on IT equipment / data
- obtaining information by deception
- human error
- inappropriate processes.

"The Review heard that near misses, hazards and insecure behaviours must all be reported without fear of recrimination, and people should be encouraged to provide this valuable intelligence."

NDG Review

In data security, staff can be your greatest asset or your greatest threat. By having an effective incident reporting system, you can help leverage the eyes and ears of your organisation and understand and learn from incidents.

An incident may involve digital and/or paper-based information. It could involve one piece of equipment or a thousand, one personal record or millions.

The incident can also be a data breach, i.e. any failure to meet the requirements of the Data Protection law, including but not limited to an unlawful disclosure or misuse of personal data. Such as when emails containing sensitive information have been sent to the wrong address, data is shared without consent, or people experience their records being misplaced or lost.

Equally, an incident may not be a breach, such as a cyber-attack that brings down a system for a short time but does not access any information or have significant negative effect on services.

The incident reporting system

There should be a uniform system for documenting any unusual problem, occurrence, or other situation that is likely to lead to undesirable effects or that is not in accordance with established policies, procedures or practices such as:

- potential and suspected disclosure of any information to unauthorised individuals
- loss or theft (attempted or actual) of paper records, data or IT equipment on which data is stored
- disruption to systems, clinical and business processes
- attempts to gain unauthorised access to computer systems, e.g. hacking
- the integrity of records altered or deleted without authorisation by the data “owner”
- virus or other malicious malware attacks (suspected or actual)
- “blagging” offence where information is obtained by deception
- breaches of physical security, e.g. forcing of doors or windows into secure room or filing cabinet containing NHS sensitive or other UK government information left unlocked in an accessible area
- leaving desktop or laptop unattended when logged-in to a user account without locking the screen to stop others accessing information
- human error, such as emailing data by mistake
- covert or unauthorised recording of meetings and presentations
- damage or loss of information and information processing equipment due to theft, fires, floods, failure of equipment or power surges
- deliberate leaking of information
- insider fraud
- systems unavailability that has a negative effect on service users / patients.

To avoid confusion and maximise the speed of response to incidents it is important that the reporting process is simple and clear.

Larger organisations may utilise a bespoke incident management IT system/software package. The information security incident process could, and should, be integrated into this. However, notwithstanding the use of a bespoke software package the principles and approach outlined here (and in Annex A) should be used to ensure the software (if utilised) and the associated processes capture the necessary information and manage the process appropriately.

Within the organisation it is suggested that the below approach is taken and tailored to the specific size and outsourced providers to the organisation:

Have a single reporting point – by telephone (essential) and email (optional addition). This reporting point should be clearly displayed on IT systems (affixed to the front of monitors for instance) and on notice boards as well as within the organisation's general operating procedures. For notice boards and operating procedures, it is recommended that a short synopsis of the types of issue that constitute an information security incident are listed to enable users to realise when an incident has occurred. This single reporting point will be required to assess the report.

Have a single, simple reporting form – this should be no more than two pages but preferably only one page, with as few questions as possible. It should be in hard copy (in case the incident affects the IT system the user is operating from) and should also be made available from the organisation's IT system/intranet. The required information is suggested to be no more than:

    - date
    - location
    - short summary of what occurred
    - type of incident – e.g. e-mail, lost USB device or paper
    - contact details for obtaining further information.

- In the plan or procedure, it should also be stated, preferably as a mandate, that all staff are responsible for reporting security incidents.

It is important that if an individual(s) has been affected by a breach that they are appropriately informed – please see Information Security Incident: NHS Digital Good Practice Guide for details Appendix 2.

Incident management system

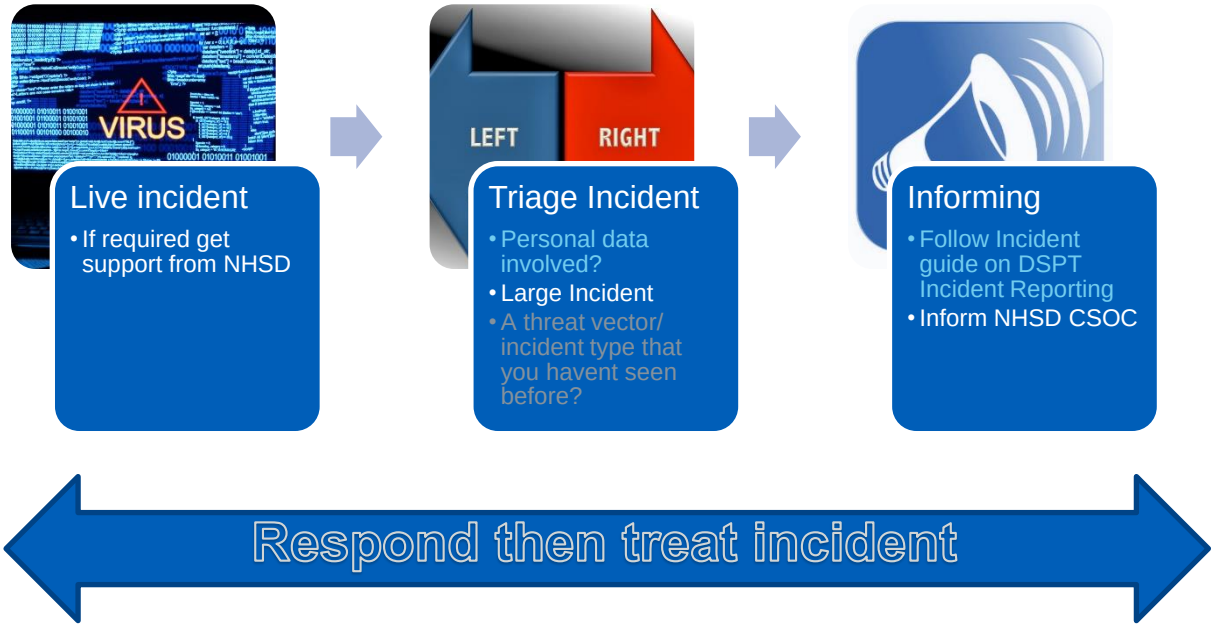
Having an incident reporting system is important however if those incidents are not managed (triaged and where appropriate investigated) lessons cannot be learned, processes and systems changed, and organisations may not improve.

Investigation

The lead investigator should not be responsible for the system or process in question. It is recognised that segregation of duties is difficult in small organisations. The same person investigating as who reported is bad practice. Where possible, the same person responsible for a system or process in focus during the investigation should not lead the investigation itself.

Managing an incident

Dependent on the nature of the incident as well as being investigated, it may need reporting to other bodies.



A policy/procedure is in place to ensure data security and protection incidents are managed/reported appropriately.

Data Security Standard 6.1.1

An informed and empowered audience

It is important that staff have sufficient knowledge to enable them to identify incidents, breaches, near misses and unacceptable behaviour and to know the tell-tale signs of what is irregular and what is acceptable behaviour.

This can be through training (as detailed in the big picture guide for data security standard 3) However organisational norms, culture, policies, processes and procedures have a profound influence.

Unsafe process (as detailed in the big picture guide for data security standard 5) can lead to more incidents and breaches.

As well as knowing what an incident / breach looks like or what a potential incident / breach could be (unsafe processes etc), staff should feel empowered and encouraged to report incidents, near misses and unsafe processes.

High levels of incident reporting in the past have often been negative and sometimes organisations have not encouraged reporting through not having a clear process and commitment to support those who report.

The NDG review heard that near misses, hazards and insecure behaviours must all be reported without fear of recrimination, and that people should be encouraged to provide this valuable intelligence. In the airline industry, spikes in incidents are seen as people following the good example set by staff speaking up about a threat, near miss or incident. Unfortunately, in health and social care, increased reporting has been perceived as an indication of systemic issues and may prompt questions around what is wrong and who is to blame.

The incident reporting system should be able to handle anonymous “tip offs” and data security whistle blowing. Many of the same principles as outlined in Sir Robert Francis, Freedom to Speak Up review (Annex A) have a bearing

- culture change
- improved handling of cases
- measures to support good practice
- particular measures for vulnerable groups
- extending the legal protection.

Consideration should be given to how the reporting system handles anonymous tip offs as well as protecting staff reporting sensitive issues that could make them vulnerable.

https://www.gov.uk/government/publications/sir-robert-francis-freedom-to-speak-up-review

This is especially a factor when incidents are reported using an existing incident reporting system, such as an IT service desk where the staff managing the incident system also manage major systems that are likely to come into focus during an incident investigation (such as a Patient Administration System or Windows Active Directory administrator).

It is recognised that this is a particular challenge for smaller organisations where staff can have multiple roles.

A Variety of Reporting routes

There is not one prescribed method of reporting incidents. Organisations may want to centralise around one prescribed route or have several valid routes.

The type of routes that are commonly used include: -

- In person
- Online form or portal (generally accessible from the local intranet)
- Leveraging an existing service desk mechanism
- Telephone line
- Central email address

Whatever the route it is important that there is appropriate level of resource available to timely triage the incident (especially if it's a live incident that requires a response) or a potential breach that may need notification with 72 hours.

Notifying Local Leaders, National Bodies and individuals of a data breach

If an incident is a potential breach (under GDPR/DPA 18) it should be triaged against the incident reporting system / guidance with the DSPT.

https://www.dsptoolkit.nhs.uk/Help/29

If the breach meets the threshold incident, details will be sent to the ICO as the supervisory authority and, dependent on impact and nature (such as a NIS breach), DHSC/NHSX

Notification needs to take place within 72 hours of you becoming aware of the breach. It is important to understand the notification system within the DSPT. It is not an incident management system (as described earlier) but a reporting tool. Once an incident has been notified, interaction will be directly with the ICO (i.e. you can't alter an existing notified incident).

In the event of a breach your board (or other equivalent leadership body) should be notified of the breach including any associated actions plans which should encompass dealing with the impact of the incidents and lessons learned (see post incident lesson learned in BPG 5 Process Reviews).

If a breach results in a high risk to the rights and freedoms of individuals the data subjects (such as patients or staff) involved will need to be informed.

See Communication of a personal data breach to the data subject (under the incident link above) and ICO guidance

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/) individuals are appropriately informed?

Is the board or equivalent notified of the action plan for all data security and protection breaches?

Data Security Standard 6.1.3

Individuals affected by a breach are appropriately informed.

Data Security Standard 6.1.4

End point anti-virus

The NDG review highlights the importance of deploying suitable measures to reduce the likelihood of incidents in the first place, such as anti-virus solutions.

Each end point (desktop computer, laptop or tablet*[1]) should be protected by an anti-virus product.

Whatever the the solution should enable you to easily determine the anti-virus status on each end-point, i.e. how up-to-date it is.updated

Your anti-virus solution will generate alerts every time an event occurs (such as a detected infected file). You should be able interrogate your system to know what they are, whether they are fixed or whether you need to take any further action.

Managing your IT estate will be easier with a central management, because even where you have a small number of endpoints, examining each one can be cumbersome. Some providers will provide you with features to manage a small estate, making this task easier.

Has antivirus/anti-malware software been installed on all computers that are connected to or capable of connecting to the Internet?

Data Security Standard 6.2.1

*[1]tablet with the main operating systems of the organisation not a mobile operating system.

Anti-virus costs

Money should not be seen as a barrier to having adequate antivirus protection. There are anti-virus packages that are bundled with the operating system (such as Microsoft Windows Defender) or can be acquired at zero or modest cost. For NHS organisations using Windows 10 (which is centrally funded) the Advanced Threat Protection version of Defender (Now known as Microsoft Defender for Endpoint (MDE)) ”is included.

Anti-virus coverage

As well as being on the endpoints, anti-virus protection should be installed on all your central infrastructure servers such as:

- File servers
- Mail servers
- application servers
- print servers.

Always on, always connected, always up to date

Antivirus / malware protection should be installed on desktops, servers, laptops and tablets*1. It includes those devices that are currently connected to the internet and those that have the capability to be connected to the internet.

The AV/Malware protection agent should be automatically updated with the latest signatures / pattern files. The updating in larger estates may be from a central source for management or smaller estates may just update from the providers themselves. In the case of ATP/MDE provided to NHS organisations as part of the centrally funded Windows 10 deployment Windows 10 rollout, updating is performed on your behalf.

Conversely not installing antivirus on a device (which supports antivirus / malware protection) should be an informed decision and effective layered controls put in place to prevent internet connection. This should be at a network level i.e. an isolated network segment and device level e.g. using non routable IP subnet range. The effect of the controls should be to mitigate the effect of accidentally connecting the device to any network with a gateway to the internet.

As well as the ability to perform a manual scan, the antivirus / malware protection should perform an automatic scan (based upon an up to date pattern/ engine) against any accessed files (irrespective of source). These can be when accessed locally, downloaded or from a network share.

Antivirus/anti-malware is kept continually up to date.

Data Security Standard 6.2.3

Antivirus/anti-malware software scans files automatically upon access.

Data Security Standard 6.2.4

Blocking web malicious content

There should be a mechanism to scan and block malicious content on web pages. This can be at the network level with internet traffic going through a web proxy, utilising the NCSC's Protective DNS (PDNS) service which blocks malicious domains or through your own block listing. Using the NHS Secure Boundary solution which implements both of these measures is recommended for those NHS organisations.

Alternatively blocking can occur at the browser level with an add on that blocks malicious content in the browser. This is generally the least favoured option in all but the smallest of organisations due to its general lack of central management.

Connections to malicious websites on the Internet are prevented.

Data Security Standard 6.2.5

Application Management

Your organisation should have an approved list of signed applications across all its platforms and devices (so called allow listing).

This applies to all types of

- Servers be that infrastructure, web and application
- Desktops and Laptops
- Tablets and Mobile Phones (with both mobile and main operating systems)

If the application is not signed or has an invalid signature it should not be executed.

You can get a code signing certificate from various suppliers and there are number of commercial and freeware tools for signing your packaged applications. (see your IT function for assistance)

Does the organisation maintain a list of approved applications, and are users prevented from installing any application that is unsigned or has an invalid signature?

Data Security Standard 6.2.7

It can be helpful to ensure devices are set up consistently though having “standard builds”. It is recognised with mobile operating systems enforcement of standard builds and applications can be challenging, however, this should not prevent the organisation having a catalogue of approved applications.

Email server software

Dependent on your organisation and whether you manage your own email system, you should have some form of ‘email gateway’ which is generally a central system that protects against these email-borne threats.

Please note, if your organisation’s mail system is NHS Mail exclusively, you do not have the requirement to monitor as this is managed on your behalf.

In addition to the requirements for server grade anti-virus and malware solutions (where appropriate and dependent on the size and structure of your organisation), it is recommended that email systems include specific features that offer additional protection, such as:

- quarantine of possibly infected files
- mass mailing protection
- secured access to logs and quarantined files for audit purposes
- generic attachment filtering
- email content and attachment inspection
- controls to prevent the forwarding of infected emails
- organisations should consider the requirement to implement controls to disallow all attachments - apart from those specified on an ‘allowed list’.This should be relatively easy to implement and maintain (e.g. what business need is there for attachment type a, b or c to be received or transmitted?).

Your chosen solution should allow reporting particularly

- volume of spam mails
- volume of emails being filtered.

Number of phishing emails reported by staff per month.

Data Security Standard 6.2.6

DMARC, DKIM and SPF

Your email service provider must implement Domain-based Message Authentication Reporting and Conformance (DMARC), Domain Keys Identified Mail (DKIM) and Sender Policy Framework (SPF) records should be implemented to make email spoofing more difficult.

DMARC should be enforced on all inbound email. These features are provided by default by NHS Mail

Spam, Spam everywhere but not a bite to eat

You should have a spam and filtering email filter in place. These can either be inbuilt with the email server product or a different third party offering.

Ultimately the goal is to reduce spam and spear-phishing. There is always a balance between how aggressive you filter spam as very low tolerance setting will lead to false positives (i.e. genuine mail being classified as spam) and vice versa.

This guide does not go into the detail of implementation (for DMARC, DKIM and SPF) as the NCSC have some comprehensive guide here

https://www.ncsc.gov.uk/guidance/email-security-and-anti-spoofing

You have implemented on your email, Domain-based Message Authentication Reporting and Conformance (DMARC), Domain Keys Identified Mail (DKIM) and Sender Policy Framework (SPF) for your organisation's domains to make email spoofing difficult.

Data Security Standard 6.2.8

You have implemented spam and malware filtering, and enforce DMARC on inbound email.

Data Security Standard 6.2.9

Acting upon known vulnerabilities

Which vulnerabilities?

There are many sources of information relating to known threats and vulnerabilities listings. For health and care organisations, the referenced authoritative list is from NHS Digital..

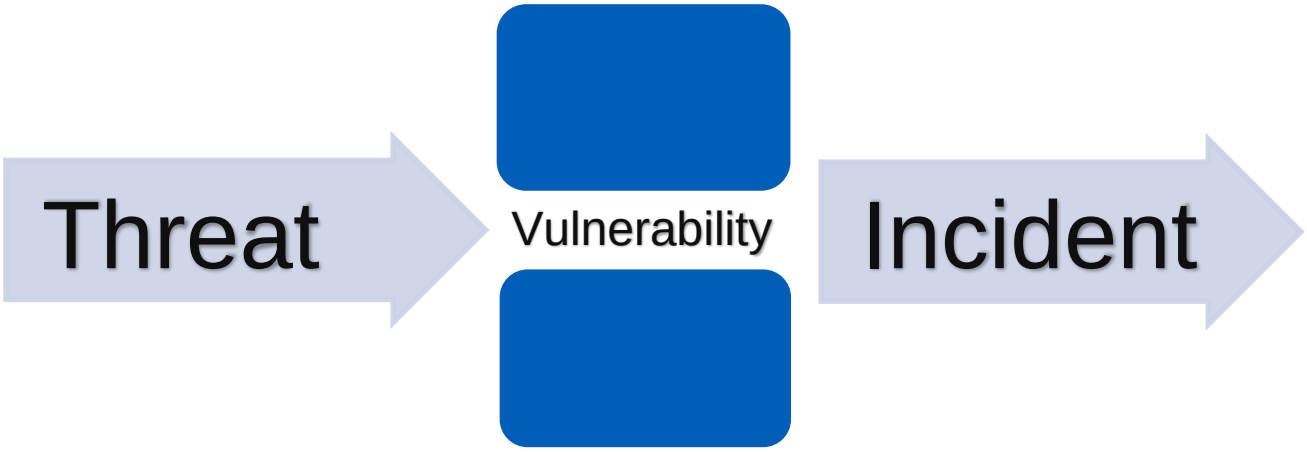
Threats and vulnerabilities are often used terms and sometime can be incorrectly interchanged.

Threats

The possible danger that could lead to an incident which could result in harm to systems and the organisation.

Vulnerability

A vulnerability is a weakness which allows an attacker to compromise security (integrity, confidentiality or availability).



A threat could exploit a vulnerability (such as a gap) to lead to a potential incident. Not every threat will have a corresponding technical vulnerability, but it is very common.

For the purpose of this guide the scope of vulnerabilities are those listed on the NHS Digital Cyber Alerts portal.

https://digital.nhs.uk/cyber-alerts

NHS Cyber Alerts Service

NHS organisations should sign up to receive Cyber alerts (see Appendix 2), once you are signed up you will receive emails alerting you of emerging threats that you need to action.

https://digital.nhs.uk/services/respond-to-an-nhs-cyber-alert

A complete repository of those threats (including vulnerabilities) is contained within NHS Cyber Alerts Portal (Appendix 2). It is important that you act upon this important intelligence. The implications of not doing so were seen during the 12th May 2017 Wannacry cyber-attacks).

Your organisation should respond to high severity cyber alerts within 48 hours. In responding to the alert include being cognisant of what the alert is asking you to do, knowing if the alert is applicable to your infrastructure and going some way in mitigating the issue.

It is recognised that some alerts mitigation will take a longer period to implement the prescribed treatment (given large estates and critical servers) however this should not be seen as an excuse for inaction.

If you have had a data security incident, was it caused by a known vulnerability?

Data Security Standard 6.3.1

The NHS Digital Data Security Centre works to make sure patient data and information is used securely and safely, through the services, guidance and support provided to health and care organisations.This includes :

- monitoring security threats to IT systems and networks and help organisations respond to these threats, through defence and incident management
- providing the national response to system-wide security incidents, such as the cyber-attack on 12 May 2017
- Working in collaboration with the National Cyber Security Centre and other arms length bodies
- offering information security consultancy and helping with security issues in system design and development
- setting and reviewing standards on IT security for the health and care sector
- providing guidance and advice for people working in health and care.

The organisation acknowledges all 'high severity' cyber alerts within 48 hours using the respond to an NHS cyber alert service.

Data Security Standard 6.3.2

Repeat data security incidents

As described earlier an incident can occur when a vulnerability is exploited. Iit is expected, hopefully prior to occurrence, that this vulnerability is treated, but certainly after the 1st occurrence.

A repeat incident is defined as an exploitation of the same vulnerability on the same systems or different ones, that occurs within 3 calendar months of the original or subsequent occurrence.

For example, an observed backdoor i.e. bypasses the system's customary security mechanisms (from the Cyber Alert portal) vulnerability in Windows Server editions.

If your trust intranet server has had a data security incident featuring the back door and the same / similar incident (similar in that it used the same back door) occurs within 3 months on the same server this qualifies under this item.

If the same back door is exploited on another server again within the 3 months leading to an incident this also qualifies.

This obviously points to practise of where possible remediating vulnerabilities across your estate before they are exploited. Where they have been exploited ensuring the same vulnerability is treated estate wide and not just on the affected system.

Have you had any repeat data security incidents within the organisation during the past twelve months?

Data Security Standard 6.3.5

Monitoring

You should be able to detect cyber events that can have an impact on your systems and services.

It is unlikely that you will have one monitoring solution in place. Monitoring and responding should be considered a multifaceted approach between people, processes and technology.

If you find the organisation has the technical capabilities to detect and log cyber events but not the people capacity to respond to them, this does not reduce your attack surface and makes you more liable to repeat data security incidents.

The NCSC has security monitoring guidance in its NIS collection

https://www.ncsc.gov.uk/collection/caf/caf-principles-and-guidance/c-1-security-monitoring

The Organisation has a proportionate monitoring solution to detect cyber events on systems and services.

Data Security Standard 6.3.3

Fraud

Increasingly digital services are proving to be attractive to cyber criminals and are being subjected to fraudulent activity.

The first step is to understand which of your digital services may be an attractive target.

Action Fraud (National Fraud and Cyber Crime Reporting Centre) has an Ato Z of fraud which should help you in identifying those systems.

https://www.actionfraud.police.uk/a-z-of-fraud-category

The focus is primarily on financial fraud, but my not be limited to that,e.g. there are identity / staff systems which could be used for identity theft or Telephony Fraud.

There is some guidance below which is the latest available (at the time of publication) however is subject to a refresh.

https://www.gov.uk/government/publications/transaction-monitoring-for-hmg-online-service-providers

Are all new digital services that are attractive to cyber criminals (such as for fraud) implementing transactional monitoring techniques from the outset?

Data Security Standard 6.3.4

Appendix 1 -
Table of Data Security Level 6 Assertions

Assertion	Sub Assertion	Evidence
6.1 A confidential system for reporting security breaches and near misses is in place and actively used.	6.1.1	A policy/procedure is in place to ensure data security and protection incidents are managed/reported appropriately.
	6.1.3	Is the board or equivalent notified of the action plan for all data security and protection breaches?
	6.1.4	Individuals affected by a breach are appropriately informed.
6.2 All user devices are subject to anti-virus protections while email services benefit from spam filtering deployed at the corporate gateway.	6.2.1	Has antivirus/anti-malware software been installed on all computers that are connected to or capable of connecting to the Internet?
	6.2.3	Antivirus/anti-malware is kept continually up to date.
	6.2.4	Antivirus/anti-malware software scans files automatically upon access.
	6.2.5	Connections to malicious websites on the Internet are prevented.
	6.2.6	Number of phishing emails reported by staff per month.
	6.2.7	Does the organisation maintain a list of approved applications, and are users prevented from installing any application that is unsigned or has an invalid signature?
	6.2.8	You have implemented on your email, Domain-based Message Authentication Reporting and Conformance (DMARC), Domain Keys Identified Mail (DKIM) and Sender Policy Framework (SPF) for your organisation's domains to make email spoofing difficult.

	6.2.9	You have implemented spam and malware filtering, and enforce DMARC on inbound email.
6.3 Known vulnerabilities are acted on based on advice from NHS Digital, and lessons are learned from previous incidents and near misses	6.3.1	If you have had a data security incident, was it caused by a known vulnerability?
	6.3.2	The organisation acknowledges all 'high severity' cyber alerts within 48 hours using the respond to an NHS cyber alert service.
	6.3.3	The Organisation has a proportionate monitoring solution to detect cyber events on systems and services.
	6.3.4	Are all new digital services that are attractive to cyber criminals (such as for fraud) implementing transactional monitoring techniques from the outset?
	6.3.5	Have you had any repeat data security incidents within the organisation during the past twelve months?

Appendix 2 - Useful resources

Security Incident Management (GPG 24): National Cyber Security Centre

Guidance on factors to consider in relation to the management of security incidents within organisations.

https://www.ncsc.gov.uk/guidance/security-incident-management-good-practice-guide-24-0

Guide to the Notification of Data Security and Protection Incidents: NHS Digital

Guidance on reporting an incident for the General Data Protection Regulation (GDPR) and Networks and Information System (NIS) Directive

https://www.dsptoolkit.nhs.uk/Help/29

Freedom to Speak Up review: an independent review into creating an open and honest reporting culture in the NHS

Sir Robert Francis publishes his report on the Freedom to Speak Up review. In his report Sir Robert sets out 20 Principles and Actions which aim to create the right conditions for NHS staff to speak up, share what works right across the NHS and get all organisations up to the standard of the best and provide redress when things go wrong in future.

http://webarchive.nationalarchives.gov.uk/20150218150512/http://freedomtospeakup.org.uk/the-report/

Professional service scheme cyber incidents: National Cyber Security Centre

An important part of business continuity and disaster recovery planning is to be prepared by identifying a supplier of Cyber Incident Response services in advance of any serious attack.

https://www.ncsc.gov.uk/scheme/cyber-incidents

Vulnerability management: National Cyber Security Centre

Guidance to help organisations assess and prioritise vulnerabilities.

https://www.ncsc.gov.uk/guidance/vulnerability-management

NHS Cyber Alerts Portal: NHS Digital

A home of cyber security alert notifications to health and care organisations, ranging from weekly threat bulletins to immediate high-severity alerts.

https://digital.nhs.uk/cyber-alerts

Data and cyber security: NHS Digital

View the latest cyber and data security policy and good practice guidance from NHS Digital's data security centre.

Sign up for security threat bulletins and emergency notifications.

https://digital.nhs.uk/cyber-security

Appendix 3 –
The National Data Guardian Reports

The NDG Report

Recommendations to improve security of health and care information and ensure people can make informed choices about how their data is used.

Review of Data Security, Consent d Opt-Outs

The government response

'Your Data: Better Security, Better Choice, Better Care' is the government's response to:

- the National Data Guardian for Health and Care's 'Review of Data Security, Consent and Opt-Outs'
- the public consultation on that review
- the Care Quality Commission's Review 'Safe Data, Safe Care'

It sets out that the government accepts the recommendations in both the National Data Guardian review and the Care Quality Commission review.

It also reflects on what we heard through consultation to set out immediate and longer-term action for implementation.

Your Data: Better Security, Better Choice, Better Care