Data Security Standard 6

Responding to incidents

The bigger picture and how the standard fits in

2023/24

Information and technology
for better health and care

Contents

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

Please refer to further note on professional judgement, auditing and UK GDPR.

https://digital.nhs.uk/cyber-and-data-security/guidance-and-assurance/data-security-and-protection-toolkit-assessment-guides/using-professional-judgement

Incident reporting (6.1.1)

Definition and scope

For the purposes of the Data Security and Protection Toolkit, an incident or breach is considered to be an adverse event that has a data protection or security implication. It can have many definitions, ranging from an IT service desk type definition to a wider business continuity incident. An incident may involve digital and/or paper-based information, and could be fairly small, affecting one personal record, or massive, affecting millions.

Incident reporting is a method or means of declaring any unusual problem, occurrence or other situation that may have (or is likely to lead to) undesirable effects, or which has violated established policies, procedures or practices.

Breaches can be grouped into three categories:

1. Confidentiality breach: the unauthorised or accidental disclosure of, or access to, personal data
2. Availability breach: the unauthorised or accidental loss of access to, or destruction of, personal data
3. Integrity breach: the unauthorised or accidental alteration of personal data

The incident reporting system (6.1.1)

Your organisation's plan or procedure should align to the Guide to the notification of data security and protection incidents. It must state all staff are responsible for reporting data protection and security incidents. An effective incident reporting system will facilitate engagement by all staff members, and learn lessons from incidents. It is important that the organisational culture enables and supports the reporting of incidents and near misses.

Incidents to be reported include any unusual problem, occurrence, or other situation that is likely to lead to undesirable effects or violates established data protection and security policy, 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, such as hacking
- altering or deleting records without appropriate authorisation
- viruses or other malicious malware attacks (suspected or actual)
- 'blagging' offences where information is obtained by deception, such as a caller impersonating a staff member or patient
- breaches of physical security, such as forcing of doors or windows into a secure room or filing cabinet containing sensitive information left unlocked in an accessible area
- leaving devices unlocked and unattended
- human error, such as emailing data by mistake
- covert or unauthorised recording of meetings and presentations
- damage or loss of information and 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 use a bespoke incident management IT system or software package. The data protection and security incident process should be integrated into this where possible. However, regardless of how incident reporting is conducted within your organisation, the process must capture the necessary information and appropriately manage the process in line with this DSPT guidance.

It is suggested that the approach below is taken and tailored to the specific size of your organisation, as well as what outsourced providers you have.

Have a single reporting point

This could be by **telephone, email or by entering onto a system.** A telephone number, or for smaller organisations, a named individual or role contact is essential so that staff can immediately raise the alarm if needed even if the IT system is down, and obtain timely advice on immediate steps to be taken. This reporting point should be clearly displayed on IT systems (affixed to the front of monitors or displayed on the front page of staff intranets for instance) and on staff notice boards, as well as within the organisation's general operating procedures. For notice boards and operating procedures, it is recommended that a short description of the types of data protection and 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 staff member cannot access the IT system the staff member is operating from) and should also be made available from the organisation's IT system or intranet. The required information is suggested to include no more than:

- date
- location
- short summary of what occurred
- type of incident – such as email, lost USB device or paper
- whether personal data has been impacted
- contact details for obtaining further information

Inform any individuals whose rights and freedoms have been severely impacted by the breach

It is important that if there is a high risk to an individual(s) rights and freedoms due to a breach, they are appropriately informed.

Please see NHS Transformation Directorate guidance on personal data breaches.

There is not one prescribed method of reporting incidents. Organisations may want to centralise around one prescribed route.

Incident management system (6.1.1)

Your organisation must have an incident management procedure that follows up on incidents after they have been reported. This ensures that, in line with the requirements in the process standard 5, lessons can be learned, processes can be improved and systems can be changed. An incident reporting system on its own is not sufficient to satisfy the requirements of the DSPT.

Investigation

The lead investigator should not be responsible for the system or process in question. It's 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, it may need to be reported to other bodies in addition to being investigated. It may need reporting to other bodies. The following steps should be taken:

1. Manage and respond the incident operationally (if appropriate) obtaining support from NHS England.
2. Follow the incident reporting guide on the Data Security and Protection Toolkit (DSPT) and inform NHS England.
3. Triage and assess the incident immediately to ensure compliance with the 72 hour reporting timeframe to the ICO if applicable. Consider whether personal data is involved, and the severity of the impact.
4. Consider whether it is a large incident - for example a threat or vector incident that you have not seen before.
5. Respond and then treat the incident. This may include applying immediate and longer term actions.

Report an incident

To report an urgent cyber security issue call 0300 303 5222.

For general data security centre queries email carecert@nhsdigital.nhs.uk.

An informed and empowered audience (6.1.1)

It is important that staff have sufficient knowledge to enable them to identify 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 Data Security Standard 3), however organisational norms, culture, policies, processes and procedures have a profound influence.

As well as knowing what an incident or breach looks like, or what a potential breach could be, staff should feel empowered and encouraged to report breaches, near misses and problem processes.

High levels of incident reporting in the past have often been perceived negatively and reporting has not been encouraged due to organisations not having a clear process and showing a lack of commitment to support individuals who report incidents.

The NDG review stated 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.

These include:

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

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.

Notifying local leaders, national bodies and individuals of a data breach (6.1.2, 6.1.3)

If an incident is a potential personal data breach (under UK GDPR/DPA 18) it should be triaged in line with the DSPT Incident Reporting Guidance and through your incident reporting system.

If the breach meets the threshold, details will be sent to the ICO as the supervisory authority and, depending on impact and nature (such as a network and information systems (NIS) breach), the Department of Health and Social Care (DHSC) or NHS England.

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 (for example, you cannot alter an existing notified incident).

In the event of a personal data breach, your board (or equivalent) should be notified of the breach including any associated action plan, which should encompass dealing with the risks and impact of the incident and lessons learned (see Standard 5 Process).

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.

You can also refer to further guidance on personal data breaches by the NHS Transformation Directorate.

End point anti-virus (6.2.1 - 6.2.9)

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 (tablet with the main operating systems of the organisation not a mobile operating system) should be protected by an anti-virus product.

Whatever the solution should enable you to easily determine the anti-virus status on each end-point, such as how often it's 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 anti-virus/anti-malware software been installed on all computers that are connected to or capable of connecting to the internet?

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 (Free of charge)

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 (6.2.3 - 6.2.4)

Antivirus or 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 antivirus or malware protection agent should be automatically updated with the latest signatures or 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, such as an isolated network segment and device level 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

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

Blocking web malicious content (6.2.5)

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 blacklisting.

Using the NHS Secure Boundary solution which implements both of these measures is recommended for 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.

Email server software (6.2.6 - 6.2.9)

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.

If your organisation’s mail system is NHSmail 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 (for example, 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.

DMARC, DKIM and SPF (6.2.8 - 6.2.9)

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 NHSmail.

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

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 (such as 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 a comprehensive guide.

Acting upon known vulnerabilities (6.3.1 - 6.3.5)

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 England.

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. Cyber vulnerabilities are listed on our cyber alerts portal.

NHS Cyber Alerts Service (6.3.2)

NHS organisations should sign up to receive cyber alerts. Once you are signed up you will receive emails alerting you of emerging threats that you need to act upon.

A complete repository of those threats (including vulnerabilities) is contained within the NHS cyber alerts portal. It's important that you act upon this important intelligence. The implications of not doing so were seen during the 12 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's 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.

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 following any recommended mitigations provided within the high severity alert.

It's recognised that some alert mitigations will take a longer to implement the prescribed remediation (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?

The NHS England 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 arm's-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
- providing table-top incident response exercises

Repeat data security incidents (6.3.5)

An multiple incident can occur when a vulnerability is exploited a number of times.

For example, if your trusts has an incident where the compromised credentials of an account of a previous employee are used by an attacker to access hospital systems.

Despite this compromise, the Leavers process is not reviewed, and then within 3 months another compromise occurs where another Leavers account which hasn't been de-activated is again exploited by a threat actor.

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 practice 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.

Monitoring (6.3.4)

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

It's 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

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

Fraud (6.3.4)

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 A to Z of fraud which should help you in identifying those systems.

The focus is primarily on financial fraud, but my not be limited to that for example there are identity or staff systems which could be used for identity theft or telephone fraud.

Organisations should consider enhancing the security controls and monitoring of areas where large financial transactions occur - such as ensuring those responsible for authoring payments have MFA on their accounts.

Appendix 1 - Useful resources

Incident management: NCSC - How to effectively detect, respond to and resolve cyber incidents.

https://www.ncsc.gov.uk/collection/incident-management

Personal data breaches: NHS England Transformation Directorate - Guidance designed to help health and care organisations deal with personal data breaches. It provides advice on what a personal data breach is and the steps that need to be taken if a breach occurs.

https://transform.england.nhs.uk/information-governance/guidance/personal-data-breaches/

Guide to the Notification of Data Security and Protection Incidents: NHS England - 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://freedomtospeakup.org.uk/

Vulnerability management: NCSC - Guidance to help organisations assess and prioritise vulnerabilities.

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

NHS Cyber Alerts Portal: NHS England - 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 England - View the latest cyber and data security policy and good practice guidance from NHS England's data security centre. Sign up for security threat bulletins and emergency notifications.

https://digital.nhs.uk/cyber

Cyber Incident Response: NCSC - The NCSC set up the Cyber Incident Response (CIR) scheme to certify companies who can help organisations who have been the victim of a significant cyber attack.

https://www.ncsc.gov.uk/information/cir-cyber-incident-response

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 and Opt-Outs

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

Your Data: Better Security, Better Choice, Better Care