Data Security Standard 6
Responding to incidents

The bigger picture and how the standard fits in
2018
Contents

Overview 3
Incident reporting system 4
  Definition and scope 4
  The incident reporting system 6
  An informed and empowered audience 8
  Incident management system 9
    Investigation 9
    Managing an incident 9
  End point antivirus 10
  Anti-virus costs 11
  Anti-virus coverage 11
  Email server software 11
  Acting upon known vulnerabilities 13
    Which vulnerabilities? 13
    Threats 13
    Vulnerability 13
  CareCERT 14
Appendix 1 - 15
  Table of Data Security Level 6 Assertions 15
Appendix 2 - 17
  Useful resources 17
Appendix 3 – 19
  The National Data Guardian Reports 19
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.”
Incident reporting system

Definition and scope

An incident can have many definitions. For the purposes of the assertions, we are interested in data security incidents.

There are three goals for data security: confidentiality, integrity and availability.

Confidentiality: When we talk about keeping information confidential, we mean that we ensure that information is not disclosed – either purposefully or accidentally – to people who don’t have the right to see it.

Most often when people talk about data breaches the type of breach is to do with confidentiality.

Integrity: When we talk about data integrity, we are talking about how we ensure that the data is accurate and unchanged. A good example is a care plan – we need to know who has inputted the information (so they are accountable for it) and also that the record is accurate.

One way of having an integrity related data security breach is when a piece of important data is intercepted when it is being sent from one place to another, the interceptor makes changes to the data, and then sends it to the intended recipient.

Availability: In order to be useful, data needs to be available to those who are authorised to see it. A breach can be caused when – either maliciously or accidentally – data cannot be accessed by those who need it. An example would be ransomware attacks on computers – a hacker locks you out of your device until you pay the ransom to have your data unlocked.

If any of these are compromised, then there is a data security incident; if the incident also involves personal confidential information, it can also be a data breach. Data breaches must be reviewed to see if the Information Commissioner’s Office (ICO) or other parties must be notified. There is more information on this below.

Incident reporting is a method or means of declaring any unusual problem, occurrence or other situation that may comprise or lead to undesirable effects, or that is not in accordance with established policies, procedures or practices. Some types of data security incident are:

- 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 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 data breach, e.g. 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 sensitive data or when sensitive data is left unlocked in an accessible area
- leaving a desktop or laptop unattended when logged-in to a user account without locking the screen to stop others accessing information
- human error, such as faxing or 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.

There are many best practices outlined in: Information Security Incident: NHS Digital Good Practice Guide Annex A.

To avoid confusion and maximise the speed of response to incidents, it is important that the reporting process is simple and clear.
Your incident reporting system should make sense for your organisation and be streamlined so that the process can be managed appropriately. In any event, at a minimum you can follow the following process:

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 and also available digitally if this makes sense for your organisation. The required information is suggested to be no more than:

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

- In the plan or procedure, it should also be stated, that all staff are responsible for reporting security incidents. They should report to the Data Protection Lead who can then investigate further. This reporting feature may be similar to your existing incident reporting procedures in other business areas.

A data security and protection breach reporting system is in place.

Data Security Standard 6.1
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. 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 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 incident reporting are seen as people follow 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.

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.

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

Users know how to spot an incident and where to report it, and incidents are effectively reported.
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

Ideally, the person who reported the incident should not be the person to investigate it. Though it is recognised that this might not be possible in very small organisations.

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

When informed of an incident the person leading the investigation should follow these steps:

- **Live incident**
  - Establish what sort of incident this is.
  - If it involves digital systems, you may need to consult with an expert for advice on how to deal with the situation.

- **Triage Incident**
  - Is personal data involved?
  - How large is the incident?

- **Informing**
  - Follow incident checklist and report via DSPT
  - Do you need to inform the data subject?
Informing

When there is a security incident, there may be instances when it is required that you report this externally.

Under the General Data Protection Regulation (GDPR) which is in force now, organisations must report any personal data breaches to the Information Commissioner’s Office (ICO) (via the Toolkit) within 72 hours. It is better to report early than to fail to report as the ICO can provide advice and guidance during your investigation.

Within the Toolkit, you can report GDPR related incidents. There is a guide on reporting an incident for the General Data Protection Regulation (GDPR) in Appendix 2 below which provides detailed information. Broadly, a GDPR incident would be any event which causes a breach of data protection law or the common law duty of confidentiality. The potential significance of the adverse effect on individuals should be reported in the reporting tool which is within this Toolkit.

If the personal data breach has a high risk of affecting a person’s rights and freedoms, then you must also let them know that their data has been breached without delay.

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 (i.e. a desktop computer, laptop or tablet*) should be protected by an anti-virus agent which is automatically updated. Some organisations which have a lot of technology may have a specific person or department with responsibility for updating the antivirus. Smaller organisations may just use the automatic updates which the antivirus software does itself.

Whatever the update route, you should know the status of the anti-virus on all of your endpoints.

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.

Your organisation may have a digital “estate”. This will include your endpoints, your server, your email system and any other digital assets you might have. An estate can vary in size from very small to huge. Managing estates will be easier with central management, because even where you have a small number of endpoints, examining each one can be cumbersome. Some IT providers will provide you with features to manage a small estate, making this task easier.

If you are not running a network, your computer, laptop or tablet should come preinstalled with antivirus software which you can use. There is more advice linked in the “resources” section below.
*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 anti-virus protection There are anti-virus packages that are bundled with the operating system (such as Microsoft Windows Defender) or which can be acquired at zero or modest cost.

**Anti-virus coverage**

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

- files
- mail
- applications
- print servers.

**Email server software**

**MANDATORY:** Number of alerts recorded by the AV tool in the last three months.

If your organisation has an email system, you should make sure that you do not send any sensitive personal information via email unless it is secure.

NHSMail is a secure email solution which is available to social care providers; there is more information available in the Resources section.

If you do not use NHSMail and would like information on how to ensure your email is secure to the right standard, then there is guidance available here: [https://digital.nhs.uk/nhsmail/secure-email-standard](https://digital.nhs.uk/nhsmail/secure-email-standard).

Email has many benefits and can improve organisation processes and efficiency. However, there are issues which arise from using email. In order to make sure you are as protected as possible there are a variety of methods you can employ: Make sure staff are trained in safe use of email, e.g. that they know how to spot phishing attacks, to be wary of attachments, and how to check if they sender if who they say they are. There is more guidance in the resources.
Your email should have a spam filter and you should make sure that all email users have robust passwords to protect access.

It may be that your organisation uses email extensively, or that you are sending personal data, if this is the case you should also implement the following technical controls. You may well need advice from a third-party. Note that if you use NHSmail, this will be monitored for you as follows:

- 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’ (or ‘whitelist’). 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 in particularly

- volume of spam mails
- volume of emails being filtered.
Acting upon known vulnerabilities

Which vulnerabilities?

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

**Threats**
A threat is what we are trying to protect against i.e. the possible danger that could lead to an incident.

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

A threat could exploit a vulnerability (such as a gap) to lead a potential incident.
CareCERT

NHS Digital’s Cyber Security Centre runs CareCERT. CareCERT alerts users to emerging threats. You should sign up to receive CareCERT alerts (see Appendix 2). The information in these alerts is often very technical and is probably of more use to your IT supplier or IT support if you have one.

The CareCERT Data Security Centre works to make sure patient data and information is used securely and safely, through the services, guidance and support we give to health and care organisations. CareCERT:

- monitors security threats to IT systems and networks and helps organisations respond to these threats, through defence and incident management
- provides the national response to system-wide security incidents, such as the cyber-attack on 12 May 2017
- works in collaboration with the National Cyber Security Centre and other arm’s length bodies
- offers information security consultancy and helps with security issues in system design and development
- sets and reviews standards on IT security for the health and care sector
- provides guidance and advice for people working in health and care
- is revising and developing a selection of services following the Government Response to the review of data-security, consent and opt-outs by National Data Guardian Dame Fiona Caldicott.

Other than the weekly email alert mentioned above, much of this functionality is only available via N3 or the Health and Social Care Network (HSCN). HSCN is available to social care providers and there is more information in the resources below. If you chose not to use HSCN, it is important that you still manage security incidents as detailed above.
## Appendix 1 -
### Table of Data Security Level 6 Assertions

<table>
<thead>
<tr>
<th>Assertion</th>
<th>Mandatory</th>
<th>Sub Assertion</th>
<th>Evidence</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.1 A confidential system for reporting security breaches and near misses is in place and actively used.</td>
<td>Yes</td>
<td>6.1.1</td>
<td>A data security and protection breach reporting system is in place.</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>6.1.2</td>
<td>List routes available for staff to report data security and protection breaches and near misses.</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>6.1.3</td>
<td>List of all data security breach reports in the last twelve months with action plans.</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>6.1.4</td>
<td>The person with overall responsibility for data security is notified of the action plan for all data security breaches.</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>6.1.5</td>
<td>Individuals affected by a breach are appropriately informed.</td>
</tr>
<tr>
<td>6.2 Users know how to spot an incident and where to report it, and incidents are effectively reported.</td>
<td>No</td>
<td>6.2.1</td>
<td>Number of security and personal information breaches reported.</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>6.2.2</td>
<td>Speed of data security and protection breach reporting.</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>6.2.3</td>
<td>Staff awareness - Reporting (Q14) - I know how to report a data security breach.</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>6.2.4</td>
<td>Number of breaches that have been reported to the Information Commissioner</td>
</tr>
<tr>
<td>6.3 All user devices are subject to anti-virus protections while email services benefit from spam filtering deployed at the corporate gateway.</td>
<td>Yes</td>
<td>6.3.1</td>
<td>Name of anti-virus product.</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>6.3.2</td>
<td>Number of alerts recorded by the AV tool in the last 3 months.</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>6.3.3</td>
<td>Name of spam email filtering product.</td>
</tr>
<tr>
<td></td>
<td>Yes</td>
<td>6.3.4</td>
<td>Number of spam emails blocked per month.</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>6.3.5</td>
<td>Number of phishing emails reported by staff per month.</td>
</tr>
<tr>
<td>No.</td>
<td>Description</td>
<td>Question/Comment</td>
<td></td>
</tr>
<tr>
<td>-----</td>
<td>------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>6.4</td>
<td>Known vulnerabilities are acted on based on advice from CareCERT, and lessons are learned from previous incidents and near misses.</td>
<td>Number and details of incidents caused by a known vulnerability being exploited.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Have you had any repeat data security incidents of the same issue within the organisation.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Staff awareness - Incidents (Q 15) - When there is a data security incident my organisation works quickly to address it.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Staff awareness - Learning Lessons (Q16) - When there is a data security incident, or near miss, my organisation learns lessons and makes changes to prevent it happening again.</td>
<td></td>
</tr>
</tbody>
</table>
Appendix 2 - Useful resources

Information Security Incident: NHS Digital Good Practice Guide

Guidance covers the considerations organisations should be taken into account, so that they can put in place good policy and procedures for dealing with information security incidents.


Care Provider Alliance

In collaboration with NHS Digital’s Social Care Programme, the CPA has started providing templates and guidance which is specific to the adult social care provider sector.


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

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


GDPR/NIS Incident Reporting Guide: 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

Anti-virus and malware guidance for health and care organisations: NHS Digital good practice guide

Guidance on good practice in using anti-virus software and protecting against malware for health and care systems and services.


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.
Vulnerability management: National Cyber Security Centre
Guidance to help organisations assess and prioritise vulnerabilities.
https://www.ncsc.gov.uk/guidance/vulnerability-management

Vulnerability scanning: NHS Digital Good Practice Guide
A guide to use of vulnerability scanners
https://nww.carecertisp.digital.nhs.uk/display/CC/Vulnerability+Scanning

CareCERT information sharing portal: NHS Digital
Only available via N3/HSCN. A home for the latest intelligence and guidance with:
- Threat Articles
- Whitepapers
- Best Practices
https://nww.carecertisp.digital.nhs.uk/

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

Health and Social Care Network: NHS Digital
https://digital.nhs.uk/health-social-care-network
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

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