NHS England

# Data Security Standard 5

## Process reviews

### 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 standard 5 states that:

*"Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security."*

Past security breaches and near misses must be recorded, and used to inform periodic workshops to identify and manage problem processes. They also allow organisations to learn lessons and prevent future breaches.

Workshops should involve looking in detail at where high risk behaviours are most commonly seen, and then considering actions to address these issues. User representation (staff within your organisation who carry out the processes) at these workshops is crucial. It is important that the impact on the user is factored into considerations of how to address these issues, as a solution which is overly taxing could result in a workaround, creating more security risks

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

# Root cause analysis (5.1.1)

Root cause analysis should be conducted routinely following a data security or protection incident, with findings acted upon.

During an ongoing incident, the top priority of your team should be resolving the problem and ensuring user data is secured and the integrity preserved. However, after the incident there will be an opportunity to investigate and review how the incident occurred.

The investigation should be thorough to determine what the root cause of the incident was and any contributory factors. This should form part of your data security and protection incident management procedure.

You should document your Investigations of root causes of issues, along with the corresponding action plans and lessons learnt. You should also keep a record of evidence associated with the agreed actions being taken to prevent similar incidents from occurring.

| Process | Issue | Lesson Learnt | Action |
|---|---|---|---|
| **Starter user account creation** | Commonly guessable passwords being used on account setup change process | There is no audit mechanism in place to check password strengths | Check other user password events such as password reset on accounts to check if guessable passwords are used |
| **Job description review** | Some contractors job descriptions do not contain data security and protection clauses | No process in place to ensure appropriate data security and protection requirements clauses are in place for contractor job descriptions | Review other contractor organisations in use to see if they comply and their job descriptions include data security and protection clauses<br>Work with Human Resources or Procurement colleagues to ensure process in place to ensure that any new contractors always have data protection clauses in their job descriptions |
| **Firewall Review Check** | On a policy based firewall “any any” rules exist | To review firewall boundary devices (especially legacy) rule set. (IPS/IDS) and DLP for any insecure rules | Remove any insecure “any any” rules |

Regardless of whether or not an incident has occurred, you should be conducting regular learning activities in the form of process reviews, simulations and business continuity exercises (as discussed in Data Security Standard 7 - Continuity planning).

Learning from your mistakes, in particular technical ones, should allow you to look at your systems, processes or controls to ensure the same incident does not occur again, or reduce the likelihood that it will.

## The difference between actions and lessons learnt

Actions tend to exist in relation to one process whereas lessons learnt can have a broader applicability. A lesson learned can have multiple actions associated with it.

# Problem processes (5.2.1)

As part of your incident root cause analysis, you may identify problems with processes in your organisation. This could be a wide variety of processes, ranging from the procedure for posting clinical letters to a firewall change rules process.

Problem processes are processes which are repeatedly linked to incidents or near misses. Processes can also be categorised as problem processes if they are linked to one high profile (or high value) incident or near miss.

All relevant stakeholders must be involved in reviewing these processes. You should also monitor these processes, ensuring that lessons are learnt, and actions are taken to improve them. The board or equivalent team should also be provided with updates and assurance, with evidence to justify the assurance.

# Appendix 1 - Useful resources

**CSED business process re-engineering methodology:** NHS Networks - A toolbox for process re-engineering.

https://www.networks.nhs.uk/

# Appendix 2 – 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