

# Data Security Standard 5

## Process Reviews

The bigger picture  
and how the standard fits in

2019/20

**Information and technology**  
**for better health and care**

# Contents

<b>Overview</b>	<b>4</b>
<b>Processes</b>	<b>5</b>
What are they?	5
Why do we do things this way?	5
What type of processes do we look at?	6
New starters access rights	6
Temporary staff access rights	6
Revoking leavers access rights	6
Staff moving roles within an organisation	6
Storage and transfer of information	6
Internet access and blocking	7
Initial boot and login times	7
Switching between users	7
Ratio of users to devices	7
Lockout times	7
Locked down devices and business applications	7
Common workarounds	8
Account sharing	8
Accounts left logged in on shared devices	8
Using a different application on the same device	8
Using an unauthorised device	8
Using elevated rights and accounts in an unfettered fashion	8
Process review	9
Example process review outputs	10
Example process: Supporting access to clinical applications for peripatetic clinicians coming into the organisation during winter pressures	10
Example attendance sheet	10
Example agenda / actions (1 <sup>st</sup> meeting)	11
Example agenda / actions (follow-up meeting)	12
An informed board	13
Lessons learnt from the process reviews	14
What's the difference between actions and lesson learnt?	15
Post Review	16
Systemic vulnerabilities	16
Improving data security and protection: learning from incidents	17
Appendix 1 -	18

---

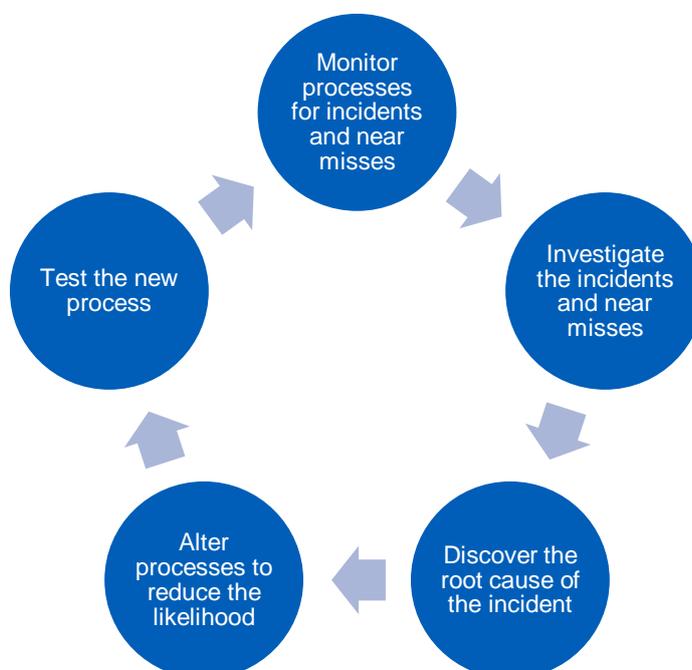
Table of data security level 5 assertions	18
Appendix 2 -	19
Useful resources	19
Appendix 3 –	20
The National Data Guardian Reports	20

## 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 are recorded and used to inform periodic workshops to identify and manage problem processes. User representation is crucial. This should be a candid look at where high risk behaviours are most commonly seen, followed by actions to address these issues while not making life more painful for users (as pain will often be the root cause of an insecure workaround). If security feels like a hassle, it's not being done properly.



# Processes

## What are they?

‘Processes’ refer to the approved procedures which users are instructed to follow when performing business functions – either using technology, paper-based information, or a combination of the two (NDG Report Appendix 1).

## Why do we do things this way?

Organisations within the care system have many processes within them. They exist for good reasons and to provide a consistent method of delivery. Some processes can however contribute to unsafe practices.

The NDG Review heard that in most cases, breaches or cyber-attacks are unwittingly facilitated by the behaviour of employees who can be classed as ‘non-malicious insiders’, primarily motivated to get their job done and often working with ineffective technologies or processes. In an evidence session held with providers, the Review heard examples of agency nursing staff being unable to access the system unless the permanent staff logged in and left the application open for the use of the agency staff. This avoidance of correct processes was the only way they could treat patients in a timely manner using the technologies available to them.

The government response to the NDG Report states that *“The processes for accessing and using systems and data – both electronic and paper based – must be robust, secure and designed with end users in mind.”*

Small changes can make a big difference, simple changes involving people and processes are often more effective than implementing expensive technological solutions; high value rather than high cost interventions.

“When processes are poorly designed or communicated, users will often revert to doing something in the most convenient way.”

**NDG Data  
Security  
Standards Report**

## What type of processes do we look at?

Each organisation will have its own local business processes and the NDG standard does not seek to mandate processes. However, there are a number of general examples of the type of processes that can be commonly attributed to incidents and workarounds. The primary focus is on digital processes however they can be paper based also.

### New starters access rights

The ability of organisations to manage the creation of new staff accounts for access to systems in a timely fashion.

### Temporary staff access rights

The ability of organisations to manage transitory staff members (such as those on staff banks) access to systems in a timely fashion.

### Revoking leavers access rights

The ability of organisations to disable / delete staff accounts who have left the organisation in a timely fashion. Particularly relevant for those staff with elevated rights to system(s).

### Staff moving roles within an organisation

There can be a tendency for staff to accumulate more rights and roles when they internally move by not having their old roles (which are no longer required) revoked.

### Storage and transfer of information

Storage and transferring of information securely and legally can be a challenge, now that consumer cloud storage and sharing is simple and free. There are safe and secure alternatives such as NHSmail and secure file transfer but invariably these tend to be more complex. It is important to inform staff of the pitfalls of using their own storage and sharing for business related information and to provide an easily accessible alternative.

## Internet access and blocking

Where an organisation has its own internet gateway, it is understood and supported that they should block malicious website and inappropriate content. However, content has to be viewed in the context of which roles are viewing it. Inflexibility and lack of granularity can lead to situations such as where pharmacies can't access drug sites, sexual health clinical staff can't access appropriate sites and psychologists can't access vulnerable service users' postings.

## Initial boot and login times

Where initial boot and login times are (or even seem) excessive, this creates an environment where there could be a tendency for some of our colleagues to find work arounds.

## Switching between users

When in a shared device environment, the ability to switch between multiple users in both the operating system and business application in a timely fashion can become critical.

## Ratio of users to devices

Where you have large number of users of a device (such as PC on a nurse station), this creates an environment where there could be a tendency for some of our colleagues to find work arounds.

## Lockout times

Where there is (or a perceived) too narrow lockout threshold for operating systems and business applications. For example, it might not be clinically safe to have a clinical application PC in an operating theatre lock after a short number of minutes. Lockout times should be granular and balance security and the operational requirements.

## Locked down devices and business applications

Where devices and applications are locked down to such a degree that reasonable operations require intervention (from an IT team) on a regular basis. Such as changing where you print to or changing your display settings.

## Common workarounds

### Account sharing

This can be due to actual (or perceived) slowness in account creation particularly for temporary staff.

### Accounts left logged in on shared devices

This can generally be attributed to a real (or perceived) slowness in switching users in both applications and operating systems.

### Using a different application on the same device

Where one application is locked (such as Internet Explorer) using a different application (such as Chrome or Firefox) might yield different results.

### Using an unauthorised device

This means using a device such as your own (which is not part of recognised Bring Your Own Device Initiative) to circumvent any lock downs. These devices can either have their own internet connection (such as any smart phone) or be connected to the corporate Wi-Fi. Use of unauthorised devices can cause issues in terms of where your business information resides (and its safety) and may provide the ability to send that information on without suitable controls.

### Using elevated rights and accounts in an unfettered fashion

Where elevated accounts' details are widely shared (especially if they also may remain unchanged over a long period) presents an opportunity for accounts to be relied upon as a workaround or inappropriately used.

## Process review

Process reviews are held at least once per year where data security is put at risk and following data security incidents.

Process reviews are held at least once per year

Data Security Standard 5.1

Where the processes involve clinicians, they are actively involved in the reviews.

It is expected that the sessions will be a frank and honest look at where processes can be improved and streamlined with a particular focus on the root causes of any workarounds. The outcomes from the process reviews will result in a list of attributable actions for attendees. These actions should be monitored, and assurance given to the [Board].

The reviews will generate a list of issues arising from the most recent review and whether they came up in previous reviews, plus reasons recorded for why they were not resolved previously. The reviews (and actions) should be agreed by the Board.

Provide summary details of process reviews held to identify and manage problem processes which cause security breaches.

Data Security Standard 5.1.2

## Example process review outputs

The following represents an example of a process review for one process (though in reality there will be multiple processes).

### Example process: Supporting access to clinical applications for peripatetic clinicians coming into the organisation during winter pressures

#### Example attendance sheet

Attendance sheet			
Process Review	Supporting access to clinical applications for peripatetic clinicians coming into the organisation during winter pressures		
Review venue	A meeting room	Date / Time	dd/mm/yy @ hh:mm
Attendees	Mrs Patricia Personnel	HR Manager	<i>Patricia Personnel</i>
	Mr Colin Cloud	IT Manager	<i>COLIN CLOUD</i>
	Miss Susan Septum	Lead Consultant	<i>SUSAN SEPTUM</i>
	Mr Lee Privilege	IG / IS Manager	<i>lee Privilege</i>
	Mrs Barbara Business	General Manager	<i>Barbara Business</i>

**Example agenda / actions (1<sup>st</sup> meeting)**

<b>Agenda / actions</b>			
Process review	Supporting access to clinical applications for peripatetic clinicians coming into the organisation during winter pressures		
Review venue	A meeting room	Date / Time	dd/mm/yy @ hh:mm
	<b>Agenda Item</b>	<b>Action</b>	<b>Allocated</b>
Agenda / actions	Honorary contracts	In order to work with us, visiting clinicians need the contractual basis resolved via an honorary contracts process	PP
Timescale		dd/mm/yy	
	Access to systems	Most of our visiting clinicians come from our neighbouring foundation trust who use the same EPR system and windows login. Investigate and report back if we can have some form of federated login for windows & EPR.	CC
Timescale		dd/mm/yy	
	Other systems	Consult with our neighbouring trust's lead consultants on what other clinical systems are required / consultant's payment for out of hours.	SS/PP
Timescale		dd/mm/yy	
	Access rights	Liaise with our neighbouring trust on having unified account settings (password complexity, longevity etc) and set an increased lockout period (20 minutes) during the winter period (Jan/Feb) in clinical areas.	LP/CC
Timescale		dd/mm/yy	

Provide a scanned copy of the process review meeting registration sheet with attendee signatures and roles held.

.....  
Data Security Standard 5.2.1

## Example agenda / actions (follow-up meeting)

Agenda / actions				
Process review	Supporting access to clinical applications for peripatetic clinicians coming into the organisation during winter pressures			
Review venue	A meeting room	Date / Time	dd/mm/yy @ hh:mm	
	Agenda Item	Action	Allocated	Status
Previous items				
Agenda / actions	Honorary contracts	In order to work with us, visiting clinicians need the contractual basis resolved via an honorary contracts process.  <i>Actions: Process produced &amp; implemented</i>	PP	Resolved
1)				
2)	Access to systems	Most of our visiting clinicians come from our neighbouring Trust who use the same EPR system and windows login. Investigate and report back if we can have some form of federated login for windows and EPR.  <i>Action: investigation complete. It is technically possible however our neighbouring trust IT department is not cooperating</i>	CC	Unresolved
3)	Other systems	Consult with our neighbouring trust's lead consultants on what other clinical systems are required / consultant's payment for out of hours.  <i>Actions : require access to PACS and lab results out of hours issues</i>	SS/PP	Resolved
4)	Access rights	Liaise with our neighbouring trust on having unified account settings (password complexity, longevity etc) and set an increased lockout period (20 minutes) during the winter period (Jan/Feb) in clinical areas.  <i>Actions : Lockout period resolved, unified setting with other</i>	LP/CC	Unresolved

List of actions arising from each process review, with names of actionees.

.....  
Data Security Standard 5.3

		neighbouring trust unresolved due to lack of cooperation		
New items				
5)	Availability of PCs	Visiting clinicians have reported problems using shared PCs due to previous user locking desktop and not logging off	CC/LP	New
Items 2 & 4 to be included in next board meeting – on dd/mm/yy @ Board Room 1				

## An informed board

As well managing your actions (such as through follow up meeting described above), it is important that the board is informed. This can be in the form of a summarised RAG report

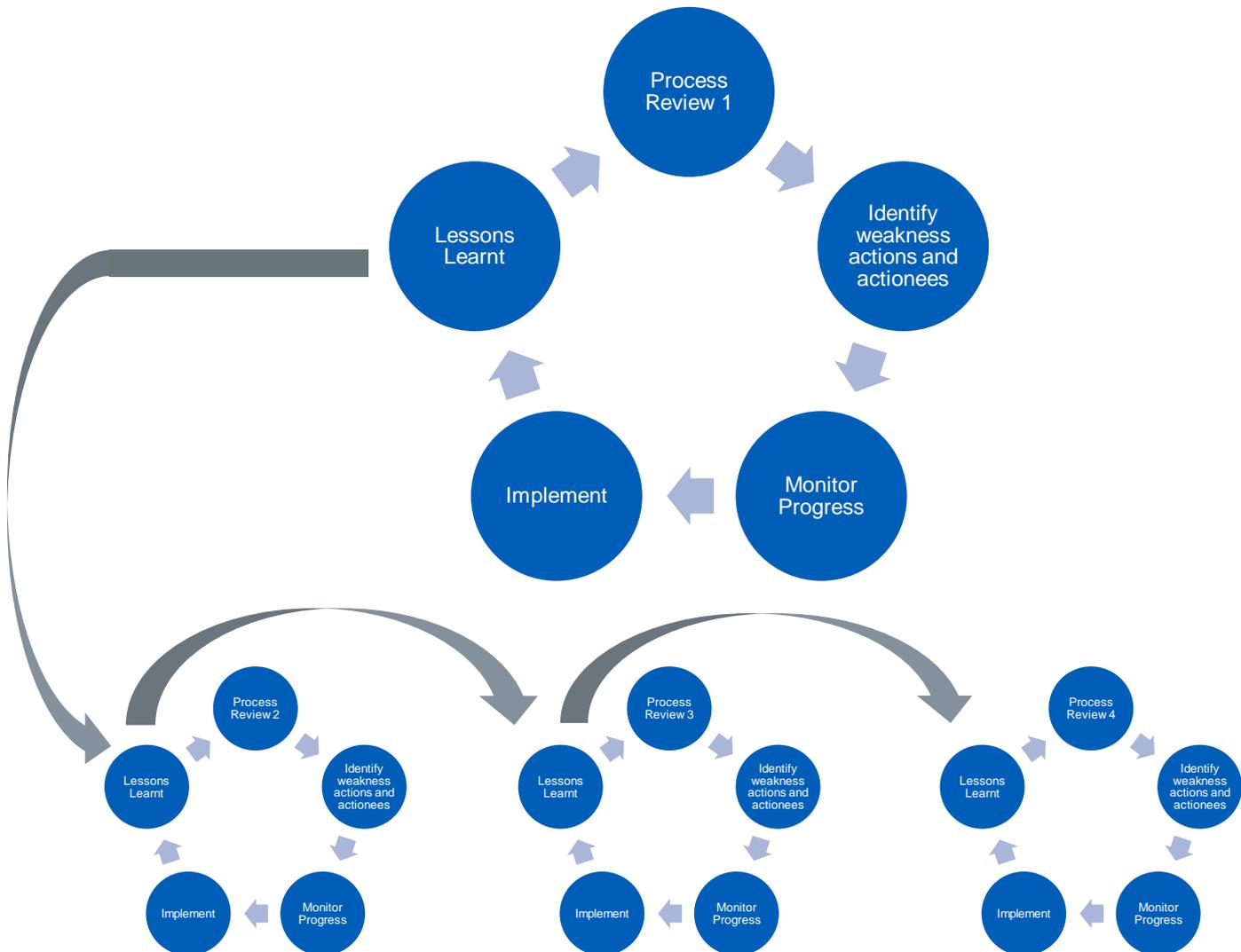
Explain how the actions to address problem processes are being monitored and assurance given to the Board or equivalent senior team?

.....  
Data Security Standard 5.3.1

(such as of the example above). This can be by exception, for example in the follow meeting the red actions (2 & 4) may be the ones you want to report to the board for their input

## Lessons learnt from the process reviews

The lesson learnt from process reviews should form part of a continuum of improvement cycles.



Completion of a process review and associated actions may result in several lessons learnt.

These lessons learnt should then be fed into other process reviews. These in turn should influence response plans for security and business continuity incidents.

## What's the difference between actions and lesson learnt?

Actions tend to exist in relation to one process whereas lessons learnt can have a broader applicability.

You use lessons learned to improve security measures, including updating and retesting response plans when necessary.

.....  
Data Security Standard 5.1.4

### Examples

Process	Action	Lesson Learnt
<b>Starter user account creation</b>	Commonly guessable passwords being used on account setup change process	Check other user password events such as password reset and account to check if guessable passwords are used
<b>Firewall review check</b>	Remove "any any" rule policies replacing with more granular ones.	Check other gateway devices IPS/IDS and DLP policy set for any insecure rules. Consider replacement with next gen firewall
<b>Job description review</b>	Some contractors job descriptions do not contacts data security and protection clauses	Review other contractor organisations in use to see if they comply (if not, do not use / ask them to change)

You should collate your lessons learnt (such as the ones in the above example) and prioritise them and action the most urgent quickly.

### Example

Priority	Lesson Learnt	Owner	Due
1	Check other gateway devices IPS/IDS and DLP policy set for any insecure rules	Colin Cloud	1/9/yy
2	Check other user password events such as password reset and account to check if guessable passwords are used	Lee Privilege	3/10/yy

Security improvements identified as a result of lessons learned are prioritised, with the highest priority improvements completed quickly.

.....  
Data Security Standard 5.1.5

<b>3</b>	Review other contractor organisations in use to see if they comply (if not, do not use / ask them to change)	Patricia Personnel	11/11/yy
----------	--	-----------------------	----------

## Post Review

### Systemic vulnerabilities

During your reviews, you may discover systemic vulnerabilities. These can range from obfuscated automated admins scripts, using older insecure software components, to systems having a password policy that allows guessable passwords.

These should be treated in the same way as lessons learnt, prioritised and actioned as soon as practicable.

Systemic vulnerabilities identified in process reviews shall be remediated as soon as practicable.

.....  
Data Security Standard 5.3.3

## Improving data security and protection: learning from incidents

As well as a process review there is a wealth of learning from real world incidents. During the incident itself there is always a focus on remediation however after the incident there is opportunity to investigate.

The investigation should be thorough to determine the root cause analysis of the incidents. This will lead to several lessons learnt that can be applied. These should be treated in the exact same way as your lessons learnt (as described earlier).

Learning from these mistakes, technical ones, should allow you to look at your system or controls to ensure the same incident does not occur again. This can be through process reviews, simulations, business continuity exercise (as discussed in the big picture 7 Continuity planning) and penetration testing.

Root cause analysis is conducted routinely as a key part of your lessons learned activities following a data security incident.

.....  
Data Security Standard 5.1.1

Post testing findings should inform the immediate future technical protection of the system or service, to ensure identified issues cannot arise in the same way again.

.....  
Data Security Standard 5.3.2

## Appendix 1 -

### Table of data security level 5 assertions

Assertion	Evidence	Evidence
<b>5.1 Process reviews are held at least once per year</b>	5.1.1	Root cause analysis is conducted routinely as a key part of your lessons learned activities following a data security incident.
	5.1.2	Provide summary details of process reviews held to identify and manage problem processes which cause security breaches.
	5.1.3	List of actions arising from each process review, with names of actionees.
	5.1.4	You use lessons learned to improve security measures, including updating and retesting response plans when necessary.
	5.1.5	Security improvements identified as a result of lessons learned are prioritised, with the highest priority improvements completed quickly.
<b>5.2 Participation in reviews is comprehensive, and clinicians are actively involved</b>	5.2.1	Provide a scanned copy of the process review meeting registration sheet with attendee signatures and roles held.
<b>5.3 Action is taken to address problem processes as a result of feedback at meetings or in year</b>	5.3.1	Explain how the actions to address problem processes are being monitored and assurance given to the Board or equivalent senior team?
	5.3.2	Post testing findings should inform the immediate future technical protection of the system or service, to ensure identified issues cannot arise in the same way again.
	5.3.3	Systemic vulnerabilities identified in process reviews shall be remediated as soon as practicable.

## Appendix 2 - Useful resources

### **NHS Networks CSED business process re-engineering methodology.**

A toolbox for process re-engineering.

[https://www.networks.nhs.uk/nhs-networks/common-assessment-framework-for-adults-learning/archived-material-from-caf-network-website-pre-april-2012/documents-from-discussion-forum/Business\\_Process\\_Re-engineering\\_BPR\\_Methodology\\_v2.2.pdf/view](https://www.networks.nhs.uk/nhs-networks/common-assessment-framework-for-adults-learning/archived-material-from-caf-network-website-pre-april-2012/documents-from-discussion-forum/Business_Process_Re-engineering_BPR_Methodology_v2.2.pdf/view)

### **NHS Improvement ACT Academy.**

Root cause analysis using five whys. Five whys was devised by Toyota as they developed their manufacturing methodologies. It forms a critical component of their problem solving training and is part of the induction into the Toyota production system. It is used in the 'analyse' phase of Six Sigma (define, measure, analyse, improve, control)

<https://improvement.nhs.uk/documents/2156/root-cause-analysis-five-whys.pdf>

### **NCSC NIS guidance**

D2. Lessons learned Learning from incidents and implementing these lessons to make a more resilient service

<https://www.ncsc.gov.uk/collection/nis-directive?curPage=/collection/nis-directive/nis-objective-d/d2-lessons-learned>

## 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

