Network & Information Systems Regulations 2018

Thresholds for Incident Reporting

Guidance

Version 2.4
2 Nov 2018

Contact email:
HealthCA@gov.scot

Website:
www.healthca.scot

Revision History:
v. 2.4 Release Document to Health Boards

Contents

1. Purpose

To present incident reporting threshold definitions and criteria for health boards to be compliant with the NIS Regulations 2018.

2. Background

The NHSS has pre-existing thresholds relating to significant information security incidents[1]. As these have been established and operational since 2014 and are familiar to health boards, it is the intention that these should be retained and expanded to incorporate compromised information systems and services consistent with the NIS Regulations.

The Network and Information Systems Regulations[2] state that Operators of Essential Services (OES) have a legal duty to notify significant incidents to the Competent Authority:

> ***The duty to notify incidents***
> ***11.***—*(1) An OES must notify the designated competent authority about any incident which has a significant impact on the continuity of the essential service which that OES provides ("a network and information systems ("NIS") incident").*

Moreover, the regulations establish requirements which the threshold criteria must incorporate:

> *(2) In order to determine the significance of the impact of an incident an OES must have regard to the following factors:*
> *(a) the number of users affected by the disruption of the essential service;*
> *(b) the duration of the incident; and*
> *(c) the geographical area affected by the incident.*

These aspects have not changed and continue to be part of the proposed criteria, with clearer examples shown in this paper.

The NIS Regulations are the overriding incident reporting requirements, however for information the Scottish Public Sector Action Plan Incident Notification Policy[3] states:

> ***Notifiable Scottish Public Sector Cyber Incidents*** *are defined as incidents or attacks against Scottish public sector network information systems which:*
> - *have the potential to disrupt the continued operation of the organisation or delivery of public services; and/or*
> - *carry a likelihood that other public, private or third sector organisations may experience a similar attack, or that the incident could spread to those organisations; and/or*
> - *could have a negative impact on the reputation of the Scottish public sector or Scottish Government; and/or*
> - *carry the likelihood of Scottish Parliament or national media interest.*

Also, the National Cyber Security Centre (NCSC) defines a "cyber incident" as follows[4]:

> *The NCSC defines a cyber security incident as:*
> - *A breach of a system's security policy in order to affect its integrity or availability*
> - *The unauthorised access or attempted access to a system*

This NCSC "cyber incident" definition is arguably too narrow for NIS regulatory purposes, whereas the Scottish PSAP definition is slightly broader in scope and thus more aligned to the NIS Regulations.

[1] Reporting Significant Information Security Incidents in NHSScotland, 12 August 2014, 11pp.
[2] Statutory Instruments, 2018 No. 506, Electronic Communications. The Network and Information Systems Regulations 2018, April 2018, 36pp. http://www.legislation.gov.uk/id/uksi/2018/506
[3] Scottish public sector cyber incident central notification and co-ordination policy. June 2018, 17pp.
[4] New Cyber Attack categorisation system to improve UK response to incidents, 12 April 2018, https://www.ncsc.gov.uk/news/new-cyber-attack-categorisation-system-improve-uk-response-incidents.

3. NIS Reporting Thresholds

3.1 Rationale

In developing NIS-compliant incident thresholds for health boards several key principles were adopted:

- **Build** on pre-existing guidance and standards
- **Minimise** complexity and change impositions on health boards
- **Align** with other incident management definitions were practicable for consistency
- Evaluation criteria should be **easy-to-understand** and capable of meaningful application in real time situations and under stress
- **Recognise** and **align** categories of "data protection" and "information systems and services" threshold criteria reporting requiremetns.

3.2 Incident Threshold Definitions

On the basis of the above, the following thresholds definitions are presented.

NOTE: In evaluating the incident category, the criterion with highest impact severity determines the incident category rating.

INCIDENT THRESHOLDS

	DATA PROTECTION	INFORMATION SYSTEMS & SERVICES
	C- Confidentiality I- Integrity A- Availability	Critical Systems & Services; Duration
1	**NEGLIGIBLE**	
	Any type of incident which may be formally recorded (e.g. on an IT reporting system), or something worthy of investigation but turns out to be a 'false positive', 'Near miss' or has negligible impact on patient privacy or services. Such information on incidents is still valuable and should be shared with local colleagues as part of normal information security planning.	**SYSTEMS**: Critical Systems & Services not involved. Key administrative IT systems not involved. **PEOPLE:** Patients: patient care not impacted. Staff: Health board staff not impacted. Population: 0%-10% local population impacted. **DURATION:** Peripheral systems and services interruption of less than a day. **GEOGRAPHY:** Impact limited to part of a health board. **REPUTATION**: No impact on the reputation of NHSS. Possible local media interest
2	**MINOR**	
	C - Confirmed or likely loss of personal data relating < 10 individuals that poses low risk to privacy (e.g. name, address, CHI and little or no clinical data which is at 'amber level') and no impact on health or safety. I - Confirmed or likely issues identified relating to integrity of up to 10 patient records such as confusing identities, out of date information or records misplaced within a Board that does not impact health but causes localised inconvenience or delays. A - Some localised and short-lived loss of services that have some minor impact on patient care.	**SYSTEMS**: Critical Systems & Services not involved; patient care not impacted. Key administrative IT systems not involved. **PEOPLE:** Patients: patient care not impacted. Staff: Health board staff not impacted. Population: 0%-10% local population impacted. **DURATION:** Peripheral systems and services interruption of more than a day but less than 5 days. **GEOGRAPHY:** Impact limited to part of a health board. **REPUTATION**: No impact on the reputation of NHSS. Possible local media interest

	3 MODERATE	
REPORTABLE INCIDENT	C - Confirmed or likely loss of personal data or privacy breach relating to 10+ individuals **OR** any highly sensitive information at 'red' level I - Issues relating to integrity 10+ individuals to the extent that the data can no longer be understood or is out of date and could have health and safety implications. A – Some disruption in service with unacceptable impact on patient care. Temporary loss of ability to provide service. **GDPR REPORTABLE**	**SYSTEMS**: Temporary loss of critical systems and services. Has the potential to disrupt the continued operation of the health board or delivery of health services. Key administrative IT systems not involved. **PEOPLE:** Patients: patient care impacted. Staff: Health board staff not impacted. Population: 0%-10% local population impacted. **DURATION:** Critical systems and services interruption and patient care disrupted for less than a day. **GEOGRAPHY:** Significant impacts widely across a health board. **REPUTATION**: Could have a negative impact on the reputation of NHSS. Possible local media interest
	NIS REPORTABLE	**NIS REPORTABLE**
	4 MAJOR	
REPORTABLE INCIDENT	C – Confirmed or likely loss of personal data or privacy breach relating to 100+ individuals **OR** loss of any sensitive personal data which is highly likely to affect the health or safety of one or more individuals. **OR** any privacy breach which because of the high profile nature of the patient(s) affected or other circumstances would lead to national media attention and significant reputational damage. I – An integrity issue which means that key data relating to 100+ patients is in effect no longer usable or understandable (and cannot be rectified) and is likely to affect health or safety. A – Sustained loss of service which has serious impact on delivery of patient care, resulting in major contingency plans being invoked. **GDPR REPORTABLE**	**SYSTEMS**: Critical systems and services failure. Key administrative IT systems performance impaired. **PEOPLE:** Patients: patient care significantly impacted. Staff: Health board staff inconvenienced. Population: 10%-50% local population impacted. **DURATION:** Critical systems and services failure interrupts continued operation of the health board(s) or delivery of health services for more than day but less than 5 days. **GEOGRAPHY:** Significant impacts across the entire health board. Wider geographic spread; likely that other health boards may experience a similar attack, or that the incident could spread to those organisations. **REPUTATION**: Local & National media interest. Negative impact on the reputation of local health board; reputation damage to NHSS
	NIS REPORTABLE	**NIS REPORTABLE**
	5 EXTREME	
REPORTABLE INCIDENT	C – Loss of data or privacy breach relating to several Boards or at national scale (i.e. 100,000+ persons or datasets on potentially all patients in Scotland); national/international media adverse publicity, prolonged damage patient/service trust and could lead to consequences to large numbers of individuals such as identity theft, financial loss etc. I – Integrity problem which leads to data on 100,000+ being unreadable or unusable and does directly lead to health and safety issues (e.g. entire data set corrupted beyond use and needs to be re-created). A – Service outage issue which leads to general failure of ICT in one or more Boards so that eHealth applications/services which are critical to the business and not running for a prolonged period. The overall business continuity of one or more Board is severely affected. **GDPR REPORTABLE**	**SYSTEMS**: Significant loss of critical systems and services. Major disruption to administrative IT systems. **PEOPLE:** Patients: patient care significantly impacted. Staff: Significant impact and inconvenience to Health board staff. Population: Over 50% local population impacted. **DURATION:** Critical systems and services failure disrupts the continued operation of the health board(s) or delivery of health services for more than 5 days. **GEOGRAPHY:** Significant impacts across the entire health board. Majority of health boards similarly impacted. **REPUTATION**: National media interest. Negative impact on the reputation of impacted health boards and on the NHSS as a whole.
	NIS REPORTABLE	**NIS REPORTABLE**

3.3 Nomenclature Definitions

The following areas are noted in the Guidance notes to Competent Authorities. These have to be defined for incident classification across the sector; for Health OES the following have been defined:

Incident Impact Definitions	Suggestions
• Systems	Critical impacts – e.g. surgical, PACS, active directory Administrative – e.g. payroll, HR.
• "user"	People = patients, staff, population
• Duration	Incident lasts <1day; >1day<5days; >5days
• Geography	<1 health board; >1 health board; > 10 health boards
• Reputation	Local media; national media interest

3.4 Incident Reporting

Incidents should be reported utilising the standard form or template current at the time. For convenience, the relevant reporting contacts are cited below.

Regulatory Obligations

GDPR Data Incident	Information Commissioners Office	casework@ico.org.uk
NIS Service Incident	Scottish Health Competent Authority	HealthCA@gov.scot

Public Sector Action Plan

"Cyber" incident	Multiple reports	The National Cyber Security Centre (NCSC)	Incidents@ncsc.gov.uk
		The Scottish Government Cyber Resilience Unit (CRU)	cyberresilience@gov.scot
		Police Scotland	cyberincident@scotland.pnn.police.uk
		SGOR	SGORRInformation@gov.scot