

|  |
| --- |
| **Incident Report NHS Scotland** |

Use this form to report an incident pertaining to an incident that has affected one or more NHS Boards in Scotland in relation to a:

* **Network Information Systems Incident (NIS)**
* **Cyber Attack**
* **UK GDPR/DPA 2018**

Once completed this report should be sent to the appropriate Digital Health and Care Divisional Office at The Scottish Government

**For NIS:** [HealthCA@gov.scot](file:///\\scotland.gov.uk\dc1\fs2_home\u414914\Significant%20Incident%20Reporting%20Guidance\HealthCA@gov.scot) with ‘**NIS Incident Report**’ in the Subject field. Personal information should not be included in this report.

**For Cyber Attack:** [HealthCA@gov.scot](file:///\\scotland.gov.uk\dc1\fs2_home\u414914\Significant%20Incident%20Reporting%20Guidance\HealthCA@gov.scot) with ‘**Cyber Attack Incident Report**’ in the Subject field. Personal information should not be included in this report.

**For UK GDPR/DPA 2018:** [DHCIG@gov.scot](mailto:DHCIG@gov.scot) with ‘**Data Breach Incident Report**’ in the Subject field. Personal information should not be included in this report.

If you decide the cyber incident requires NCSC's support (for action) or is for wider interest (for information). Then as an Operator of Essential Services (OES) under the NIS Regulations, go to <https://report.ncsc.gov.uk> and use their form to alert NCSC.

You may have to notify two separate regulators about the same incident – NIS Competent Authority and the ICO (if the same incident is also a personal data breach). You must make both notifications without undue delay and within 72 hours of becoming aware, where feasible.

|  |  |
| --- | --- |
| **Significant Information Security Incident Report NHSScotland** | |
| Incident Name |  |
| Date/Time/Duration of Incident |  |
| Reporting Officer –  Role, contact details |  |
| Ongoing point of contact if different from Reporting Officer - Name, role, email, phone etc. |  |
| Your NHS Board |  |

|  |  |
| --- | --- |
| **Report Type** | |
| Initial Report |  |
| Follow Up Report |  |

|  |  |
| --- | --- |
| **Incident Details** | |
| Incident type:   * NIS – Loss of Service * Cyber Attack * Data Brach - UK GDPR/DPA 2018 * Other |  |
| Brief description of incident |  |
| How did this incident occur |  |
| How was this incident discovered |  |
| Was personal information involved? If so, provide number and type of information. |  |
| Number of people/users affected |  |
| Geographical area affected |  |
| What preventative measures were in place |  |
| Has Business Continuity been invoked and what form does this take |  |
| Has the Incident been resolved |  |
| Do you have an internal ID for the incident |  |

|  |  |
| --- | --- |
| **Description of Impact** | |
| Briefly describe the impact in terms of confidentiality, integrity, and availability of information |  |
| Describe any impact on patient care |  |
| information concerning any, or any likely, cross-border impact of a NIS incident |  |
| Impact level (MODERATE, MAJOR, or EXTREME) |  |

|  |  |
| --- | --- |
|  | **Awareness** |
| Has the NCSC been informed |  |
| Has the ICO been informed |  |
| If this is a data breach, have data subjects been informed Yes/No/Pending investigation |  |
| Who else has been informed | e.g., NSS, partners/other data controllers/ Other areas within Scottish Gov. etc. |

|  |  |
| --- | --- |
| **Media Involvement** | |
| Is there media involvement? |  |
| If Yes, provide copy of the media statement |  |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |
| --- | --- |
| **Contacts** | |
| Have you reported to all relevant parties? | CA - [HealthCA@gov.scot](mailto:HealthCA@gov.scot)  NCSC - <https://report.ncsc.gov.uk>  ICO - <https://ico.org.uk/for-organisations/report-a-breach/>  Digital Health and Care Information Governance [DHCIG@gov.scot](mailto:DHCIG@gov.scot)  **Out of Hours:**  The Scottish Government Cyber Resilience Unit (CRU): 0300 244 4000, ask for CRU Duty Officer |

|  |  |  |
| --- | --- | --- |
|  | **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 minimal 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 ten 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. | **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 |
| **GDPR REPORTABLE** |
| **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. | **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 |
| **GDPR REPORTABLE** |  |
| **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. | | **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. | |
| **GDPR REPORTABLE** | |  | |
| **NIS REPORTABLE** | | **NIS REPORTABLE** | |

**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 |
|  |  |