Information Governance Incident Response Plan

Policy Title:	Information Governance Incident Response Plan
Policy Group:	Information Governance and Administration
Policy Owner:	Information Services Manager
Issue Date:	April 2021
Review Period:	12 months
Next Review Due	April 2022
Author:	Simon Burchell, Information Service Manager (SIRO)
Cross References:	Information Governance Policy, Business Continuity Policy, Business Continuity Plan
Evidence:	NHS Digital Data Protection and Security Toolkit
How implementation will be monitored:	Observations when some incident occurs (e.g. virus infection, unplanned service interruption) and by review with managers in respect of specific threats
Computer File Ref.	O:\risk management\Policies\Information Governance and Administration
Policy Accepted by MT	7th April 2021
Sign-off by CEO	

This Incident Response Plan is documented to provide a well-defined, organised approach for handling any potential threat to computers and data, as well as taking appropriate action when the source of the intrusion or incident at a third party is traced back to the Holy Cross Hospital private network. This Incident Response Plan identifies and describes the roles and responsibilities of the Incident Response Team. The Incident Response Team is responsible for putting the plan into action.

A copy of this plan will be kept in the red Business Continuity folder by the fire panel in Reception.

Incident Response Team

The Incident Response Team is established to provide a quick, effective and orderly response to computer related incidents such as virus infections, hacker attempts and break-ins, improper disclosure of confidential information to others, system service interruptions, breach of personal information, and other events with serious information security implications.

The Incident Response Team's mission is to prevent a serious interruption to patient care, loss of profits, client confidence or access to information assets by providing an immediate, effective and skilful response to any unexpected event involving computer information systems, networks or databases.

The Incident Response Team is authorised to take appropriate steps deemed necessary to contain, mitigate or resolve a computer security incident. The Incident Response Team is responsible for investigating suspected intrusion attempts or other security incidents in a timely, cost-effective manner and reporting findings to management and the appropriate authorities as necessary. The Information Services Manager will coordinate these investigations.

Unless otherwise instructed, each plan recipient will receive and maintain two copies of the plan, stored as follows:

- One copy at the plan recipient's office
- One copy at the plan recipient's home

For additional copies, contact the Information Services Manager

Incident Response Team Members

Information Services Manager (SIRO)
Chief Executive
General Manager
Learning and Development Coordinator (DPO)

Incident Response Team Notification

For ease of reporting, and to ensure a timely response 24 hours a day, seven days a week, the Information Services Manager will act as the central point of contact for reporting any incidents. In the absence of the Information Services Manager, the Learning and Development Coordinator will act as his deputy, and first point of contact.

All computer security incidents reported to the IT contractor Help Desk must be reported to the Information Services Manager. A preliminary analysis of the incident will take place by the Information Services Manager that will determine whether Incident Response Team activation is appropriate.

Types of Incidents

There are many types of information governance incidents that may require Incident Response Team activation. Some examples include:

- Breach of personal information
- Denial of service/Distributed denial of service
- Excessive port scans
- Firewall breach
- Virus outbreak

Breach of Personal Information — Overview

This Incident Response Plan outlines steps the Hospital will take upon discovery of unauthorised access to personal information on an individual that could result in harm or inconvenience to the individual such as fraud or identity theft. The individual could be either a patient or employee of Holy Cross Hospital.

Personal information is information that is, or can be, about or related to an identifiable individual. It includes any information that can be linked to an individual or used to directly or indirectly identify an individual. Most information the firm collects about an individual is likely to be considered personal information if it can be attributed to an individual.

Personal information is defined as any of the following types of information that individually or combined, may result in the identification of an individual.

- Name
- Identification number (such as NHS Number, Hospital Number, National Insurance Number, Driver's License Number, Passport Number etc.)
- Medical or health information
- Financial details
- Home address or e-mail address
- Racial or ethnic origin
- Political or trade union activities
- Religion
- Criminal record

Definitions of a Security Breach

A security breach is defined as unauthorised acquisition of data that compromises the security, confidentiality or integrity of personal information maintained by Holy Cross Hospital. Good faith acquisition of personal information by an employee or agent of our company (e.g. a volunteer or contractor) for business purposes is not a breach, provided that the personal information is not further used or subject to unlawful use or further unauthorised disclosure.

Employee Responsibilities

All Hospital employees must report any suspected or confirmed breach of personal information on to the Information Services Manager (SIRO) or Learning & Development Coordinator (Data Protection Officer) immediately upon discovery. This includes notification received from any third- party service providers or other business partners with whom the organization shares personal information on individuals.

The employee reporting the suspected breach will assist in acquiring information, preserving evidence and providing additional assistance as deemed necessary by the Information Services Manager or other Incident Response Team members throughout the investigation.

Classification / Identification of a Potential Incident

All reports of a potential incident shall be classified as a high/medium/low risk to facilitate the actions to take.

Criticality: High
Definition: Incidents that have a monumental impact on the Hospital's business or service to patients.
Example: Unauthorized system access.

Criticality: Medium
Definition: Incidents that has a significant or has the potential to have a monumental impact on the firm's business or service to its clients. Example: Password cracking attempt.

Criticality: Low
Definitions: Incidents that has the potential to have a significant or monumental impact on the firm's business or service to its clients. Example: Firewall scanning.

Response

Once a potential incident has been reported, the Information Services Manager or Learning and Development Coordinator should be notified for response. The Information Services Manager or Learning and Development Coordinator will be responsible for performing the initial investigation to determine if an incident has occurred. The following checklist identifies steps that can be used to facilitate in classifying the incident, if one in fact has occurred:

- Malware scans
- Collection and review of log files
- Review of installed or running privileged programs
- Inspection for system file tampering
- Network Monitoring Programs reports
- Detection of unauthorised services installed on systems
- Evidence of password file changes
- Review system and network configurations
- Detection of unusual files

Note: In responding to a reported incident, it may be prudent to shut down any or all systems for the stopping of an attack in real time and/or the preservation of any potential forensic evidence.

Recovery

The main purpose of this Incident Response Plan is to ensure an efficient recovery through the eradication of security vulnerabilities and the restoration of repaired systems. Recovery includes ensuring the attacker's point of penetration and any associated vulnerabilities have been eliminated and all system operations have been restored.

Periodic Testing & Remediation

It is the responsibility of the Information Services Manager to review the Incident Response Plan annually. When testing is done, each system should be scanned for the open vulnerability before remediation and then scanned again after the remediation to verify that the vulnerability has been eliminated. For example, antivirus scans should be run a number of times – if a virus is intercepted by the scan, further scans should be run to ensure that it has been removed.

Incident Response Plan

This document discusses the steps taken during an incident response plan**.**

1) Anyone who discovers the incident will contact the Information Services Manager or his deputy. They will log on the IT database:

   a. Name of caller or source of incident alert (software notifications).
   b. Time of first report.
   c. Nature of the incident.
   d. What system(s) or persons were involved?
   e. Location of equipment or persons involved.
   f. How incident was detected.

2) The Information Services Manager or his deputy will be the first line of response. Most incidents will be highly localised and rapidly contained.

3) Where the Information Services Manager or his deputy are unable to resolve the incident, it will be referred onwards to the relevant contractor via their normal helpdesk route.

4) In the event of a serious incident, the Information Services Office, and will contact those designated on the Incident Response Team list. The Information Services Office will log the information received, and add the following information to the report, where relevant:

   a. Is the equipment affected business critical?
   b. What is the severity of the potential impact?
   c. Name of systems being targeted, along with operating system, IP address, and location.
   d. IP address or any other information about the origins of the incident.

5) Contacted members of the response team will meet or discuss the situation over the telephone and determine a response strategy.

   a. Is the incident real or perceived?

   b. Is the incident still in progress?

   c. What data or property is threatened and how critical is it?

   d. What is the impact on the business should the attack succeed? Minimal, serious, or critical?

   e. What system or systems are targeted, where are they located physically and on the network?

   f. Is the incident inside the trusted network?

   g. Is the response urgent?

   h. Can the incident be quickly contained?

   i. Will the response alert the attacker and do we care?

j. What type of incident is this? Example: virus, worm, intrusion, abuse, damage, data breach.

6) The relevant IT contractor will be contacted and an incident ticket will be created. For network related incidents, the contractor is Virtual IT. The incident will be categorised into the highest applicable level of one of the following categories:

   a. High - Incidents that have a monumental impact on the Hospital's business or service to patients.
   b. Medium - Incidents that have a significant impact, or have the potential to have a monumental impact on the Hospital's business or service to its patients.
   c. Low - Incidents that have the potential to have a significant or monumental impact on the firm's business or service to its clients.

7) The Information Services Manager, with the assistance of relevant IT contractors where necessary, will use investigative techniques, including reviewing of system logs, looking for gaps in logs, reviewing intrusion detection or firewall logs and interviewing witnesses to determine how the incident was caused. Only authorised personnel should be performing interview or examining IT systems. Informal interviews will be limited to the Information Services Manager or his deputy asking what happened. Formal interviews that may involve challenge staff actions will only be carried out with the involvement of Human Resources. A chain of custody must be established and all potential evidence preserved and secured for turnover to proper authorities if required.

8) The Incident Response Team will recommend changes to prevent the occurrence from happening again or spreading to other systems.

9) The Information Services Office will restore the affected system(s) to the pre-incident state and assess potential damages. When necessary, this will involve the support of one or more contractors such as Virtual IT (main IT support), or dedicated 3rd-party software support lines (Exchequer, TM3, Access Payroll etc.).

10) Information breaches will be measured against the NHS Digital/ICO reporting tools and, when necessary, reported to the relevant regulator.

11) There will be a post-mortem review of the response and policies will be updated where necessary – take preventive steps so the incident doesn't happen again.

   a. Would an additional policy, or modification to a policy, have prevented the incident?
   b. Was a procedure or policy was not followed which allowed the incident? What could be changed to ensure that the procedure or policy is followed in the future?
   c. Was the incident response appropriate? How could it be improved?
   d. Was every appropriate party informed in a timely manner?
   e. Were the incident-response procedures detailed and did they cover the entire situation? How can they be improved?
   f. Have changes been made to prevent another incident? Have all systems been patched, systems locked down, passwords changed, anti-virus updated, email policies set, etc.?
   g. Should any security policies be updated?
   h. What lessons have been learned from this experience?

Information Incident Response Team contact details

Simon Burchell	Information Services Manager (SIRO)	07792 146337
Joanna Phillips	L&D Coordinator (DPO)	07747 322759
Joanna Speed	General Manager	07766 734809
Ross White	CEO	07751 303047

Contractor Helpline contact details

Virtual IT	Main IT support (server & network)	020 7644 2820
Exchequer	Accounts software support line	03301 224 402
Access Payroll	Payroll software support line	01206 321446 (A/C RH327)
TM3	Outpatients management system	03333 442 800
Paralogic	Website hosting support, education broadband line	0330 122 1000

Regulator contactor details

Information Commissioner’s Office	Breach reporting helpline	0303 123 1113
NHS Digital	Cyber security reporting	0300 303 5222

Basic malware response

1. Disconnect infected machine from network.
2. Install latest version of MalWareBytes free version via approved USB flash drive.
3. Scan with MalWareBytes, and clean.
4. Scan with Webroot, and clean.
5. If necessary, use additional malware removal tools.
6. Rescan with MalWareBytes and Webroot after each cleaning operation, and reboot.
7. Machine not considered clean until 2 consecutive clean scans with both products (i.e. 4 clean scans in total).
8. If malware proves highly resistant to removal, escalate to Virtual IT, who provide our Webroot anti-malware product. Highly-resistant malware can require complete operating system reinstallation.

Appendix 1: Reporting to the Information Commissioner's Office

When a personal data breach has occurred, you need to establish the likelihood and severity of the resulting risk to people's rights and freedoms. If it's likely that there will be a risk then you must notify the ICO; if it's unlikely then you don't have to report it. However, if you decide you don't need to report the breach, you need to be able to justify this decision, so you should document it.

In assessing risk to rights and freedoms, it's important to focus on the potential negative consequences for individuals. A breach can have a range of adverse effects on individuals, which include emotional distress, and physical and material damage. Some personal data breaches will not lead to risks beyond possible inconvenience to those who need the data to do their job. Other breaches can significantly affect individuals whose personal data has been compromised. You need to assess this case by case, looking at all relevant factors.

So, on becoming aware of a breach, you should try to contain it and assess the potential adverse consequences for individuals, based on how serious or substantial these are, and how likely they are to happen.

For more details about assessing risk, please see section IV of the Article 29 Working Party (WP29) guidelines on personal data breach notification. WP29 has been replaced by the European Data Protection Board (EDPB) which has endorsed these guidelines.

Appendix 2: Reporting to NHS Digital

Grading the personal data breach

Any incident must be graded according to the significance of the breach and the likelihood of those serious consequences occurring. The incident must be graded according to the impact on the individual or groups of individuals and not the organisation. It is advisable that incidents are reviewed by the Data Protection Officer or Caldicott Guardian or the Senior Information Risk Owner when determining what the significance and likelihood a data breach will be.

The significance is further graded rating the incident of a scale of 1-5. 1 being the lowest and 5 the highest.

The likelihood of the consequences occurring are graded on a scale of 1-5 1 being a non- occurrence and 5 indicating that it has occurred.

Where the personal data breach relates to a vulnerable* group in society, as defined below, the minimum score will be a 2 in either significance or likelihood unless the incident has been contained. This will have the effect of automatically informing the Information Commissioner if one of the other axes scores above a 3.

*Where vulnerable is a 'Child known to safeguarding or with mental health conditions. Adult with capacity issues or known to adult safeguarding'.

Establish the likelihood that adverse effect has occurred

No.	Likelihood	Description
1	Not occurred	There is absolute certainty that there can be no adverse effect. This may involve a reputable audit trail or forensic evidence
2	Not likely or any incident involving vulnerable groups even if no adverse effect occurred	In cases where there is no evidence that can prove that no adverse effect has occurred this must be selected.
3	Likely	It is likely that there will be an occurrence of an adverse effect arising from the breach.
4	Highly likely	There is almost certainty that at some point in the future an adverse effect will happen.
5	Occurred	There is a reported occurrence of an adverse effect arising from the breach.

If the likelihood that an adverse effect has occurred is low and the incident is not reportable to the ICO, no further details will be required.

Grade the potential severity of the adverse effect on individuals

No.	Effect	Description
1	No adverse effect	There is absolute certainty that no adverse effect can arise from the breach
2	Potentially some minor adverse effect or any incident involving vulnerable groups even if no adverse effect occurred	A minor adverse effect must be selected where there is no absolute certainty. A minor adverse effect may be the cancellation of a procedure but does not involve any additional suffering. It may also include possible inconvenience to those who need the data to do their job.
3	Potentially some adverse effect	An adverse effect may be release of confidential information into the public domain leading to embarrassment or it prevents someone from doing their job such as a cancelled procedure that has the potential of prolonging suffering but does not lead to a decline in health.
4	Potentially Pain and suffering/ financial loss	There has been reported suffering and decline in health arising from the breach or there has been some financial detriment occurred. Loss of bank details leading to loss of funds. There is a loss of employment.
5	Death/ catastrophic event.	A person dies or suffers a catastrophic occurrence

Both the adverse effect and likelihood values form part of the breach assessment grid.

There are a limited number of circumstances where, even when an organisation is aware of a breach of personal data, there may be containment actions that will remove the need for notification to the ICO but may still need to be recorded as a near miss as it may still constitute a reportable occurrence under the NIS directive.

Under the following circumstances notification may not be necessary;

- encryption – where the personal data is protected by means of encryption.
- 'trusted' partner - where the personal data is recovered from a trusted partner organisation.
- cancel the effect of a breach - where the controller can null the effect of any personal data breach.

Breach Assessment Grid

This operates on a 5 x 5 basis with anything other than "grey breaches" being reportable. Incidents where the grading results are in the red are advised to notify within 24 hours.

Severity (Impact)	Catastrophic	5	5	10	15	20	25
						DHSC & ICO	
	Serious	4	4	8	12	16	20
	Adverse	3	3	6	9	12	15
						ICO	
	Minor	2	2	4	6	8	10
	No adverse effect	1	1	2	3	4	5
			1	2	3	4	5
			Not Occurred	Not Likely	Likely	Highly Likely	Occurred
			Likelihood that citizens' rights have been affected (harm)				