NHS Improvement

15 August 2016

Wellington House
133-155 Waterloo Road
London SE1 8UG

T: 020 3747 0000
E: nhsi.enquiries@nhs.net
W: improvement.nhs.uk

[redacted]

By email [redacted]

Dear [redacted]

Request under the Freedom of Information Act 2000 (the "FOI Act")

I refer to your email of **23 July 2016** in which you requested information under the FOI Act from NHS Improvement. Since 1 April 2016, Monitor and the NHS Trust Development Authority (NHS TDA) are operating as an integrated organisation known as NHS Improvement. For the purposes of this decision, NHS Improvement means Monitor and NHS TDA.

Your request

You made the following request:

"1. Does your organisation have a cyber abuse or cyber trolling/bullying or social media policy - or a related policy such as Bullying and Harassment or Internet Usage - where cyber abuse or cyber bullying is mentioned? If so can I request a copy?

2. Have any staff at your organisation (names or specific details are not needed) - been disciplined or suspended, or their employment terminated due to anything related to cyber abuse, social media conduct, cyber bullying, internet usage, or bullying and harassment by electronic means?"

Decision

NHS Improvement holds the information that you have requested and has decided to release this.

Question 1

NHS Improvement has an "Information Governance Incident Management and Reporting Procedure", which explains how incidents, including cyber bullying and disclosing information on social media, should be reported and managed. As the document explains, this procedure is designed to ensure incidents are reported, recorded and investigated by encouraging an open, honest and immediate reporting system. Section 2 of the Procedure provides the process for logging, managing, investigating, reporting and then closing an incident relating to cyber security. I have attached a copy of this Procedure to this response.

Question 2

I note that no time period was provided in your request. Monitor was established in 2004 and NHS TDA in 2013. To conduct a formal search of all records would be an extensive task that would likely exceed the appropriate limit on the cost of compliance with a request, as provided by the FOI Act. However I have spoken to colleagues who have worked within the human resources teams at Monitor and NHS TDA for several years and have knowledge of specific cases and general oversight of HR issues, in the expectation that this should satisfy your request.

We have identified three cases within the ambit of your request where a formal disciplinary investigation was commenced. Two of these cases related to suspected abuse of internet usage and one related to alleged harassment, in which email communications were part of the material investigated. Of these cases, two involved both suspension and termination of employment. The other case was formally investigated but did not involve suspension or result in termination of employment.

Review rights

If you consider that your request for information has not been properly handled or if you are otherwise dissatisfied with the outcome of your request, you can try to resolve this informally with the person who dealt with your request. If you remain dissatisfied, you may seek an internal review within NHS Improvement of the issue or the decision. A senior member of NHS Improvement's staff, who has not previously been involved with your request, will undertake that review.

If you are dissatisfied with the outcome of any internal review, you may complain to the Information Commissioner for a decision on whether your request for information has been dealt with in accordance with the FOI Act.

A request for an internal review should be submitted in writing to FOI Request Reviews, NHS Improvement, Wellington House, 133-155 Waterloo Road, London SE1 8UG or by email to nhsi.foi@nhs.net.

Publication

Please note that this letter and the attached information will shortly be published on our website. This is because information disclosed in accordance with the FOI Act is disclosed to the public at large. We will, of course, remove your personal information (e.g. your name and contact details) from the version of the letter published on our website to protect your personal information from general disclosure.

Yours sincerely,

Sophie Ellis
Senior ER Manager

NHS Improvement

Information Governance Incident Management and Reporting Procedure

Document Control Information

Policy Owner

Name	Role / Title
Pete Sinden	Monitor CIO

Author

Name	Role / Title
Kirsty Benn-Harris	Information Governance Manager

Reviewed and Approved By

Name	Role	Date
Elizabeth Dimond **Amanda Downes** **Kathy McLean** **Alison Walne** **Richard Wilson**	**IG Representatives from NHSI**	11 May 2016

Version History

Version No.	Version Date	Revised By	Affected Section & Description of Change
1.0	16.06.2016	KBH	First draft of this procedure for NHSI purposes. Policy to accompany other policies e.g. Information and Data Handling Policy & Information Security and Cyber Security Policy
1.1	14.07.2016	KBH	Updated after Legal review

Date of Next Review: Jan 2017

1. GENERAL GUIDANCE AND REQUIREMENTS FOR REPORTING OF INCIDENTS

1.1. Introduction

To ensure that NHS Improvement (NHSI) minimises the damage from Information Governance (IG) or cyber security related incidents and learns from them, it must ensure all incidents are reported, recorded and investigated.

All members of staff are required to report any observed or suspected incident, including weaknesses identified in systems design or operational procedures, which are likely to give rise to an incident.

NHSI encourages an open, honest and immediate reporting system that is used to improve practice and reduce risk. All members of staff have a responsibility to report such incidents.

1.2. Scope

This procedure applies to all staff (regardless of their place of work) that carries out work within or on the behalf of NHSI.

For the purposes of this procedure, an information security incident is a suspected, attempted, successful, or imminent threat of unauthorized access, use, disclosure, breach, modification, or destruction of information; or significant violation of Information Governance and Information and Data Handling policy. A cyber related or any malicious act or suspicious event that attempts to compromise or disrupt NHSI IT networks.

A Serious Incident Requiring Investigation (SIRI) is related to the loss of personal data and/or any information that could lead to identity fraud or have other significant impact on individuals or the organisation.

The definitions apply to both electronic media and paper records.

1.3 Purpose

The purpose of this procedure is to familiarise staff with the reporting arrangements for suspected, actual or near miss IG and security incidents which occur within or in relation to the works carried out at NHSI.

This procedure should be used in conjunction with, but not limited to national guidance, the guidance issued by NHS Digital on the management of IG and Cyber Security Serious Incidents and the following NHSI policies:

- Information Governance Framework - Policy and Strategy
- Email, Internet and Telecommunications Policy
- Information and Data Handling Policy
- Information Security and Cyber Security Policy

The intention is to ensure that:

- The management of incidents conforms with the processes and procedures set out for managing all such incidents
- There is a consistent approach to evaluating incidents
- Early reports of an incident are sufficient to decide appropriate escalation, notification and communication to interested parties
- Appropriate action is taken to prevent damage to the public, staff and the reputation of NHSI or its partner organisations
- All aspects of an incident are fully explored and any lessons learnt are identified and communicated across the organisation
- Appropriate corrective action is taken to prevent recurrence

1.4. Identifying incidents

1.4.1. What is a reportable IG or cyber security incident?

An incident can generally be described as an event which has or could lead to a breach of confidentiality, legislation or regulation, operations, policy or security.

Some **common examples** of IG and cyber security incidents are listed below:

- Loss of personal computer and other company equipment which holds Personal Identifiable Data (PID) or other sensitive information
- Access to inappropriate websites in breach of the NHSI Email, Internet and Telecommunications policy
- Theft of equipment and/or data
- A computer virus
- Successful hacking attack
- Accessing a system or computer using someone else's authorisation either fraudulently or by accident
- Finding misplaced sensitive information outside of NHSI premises
- Sensitive information sent to a third party by insecure means

Some examples of an **IG SIRI**:-

- This type of incident will typically breach one or more of the data protection principles in the Data Protection Act 1998 and/or the Common Law Duty of Confidentiality
- This includes unlawful disclosure or misuse of confidential data, failing to address a known inaccuracy in records containing personal data, inadequate data security measures and unfair invasion of an individual's privacy

A Cyber-related SIRI is anything that could (or has) compromised information assets within Cyberspace. Cyberspace is an interactive domain made up of digital networks that is used to store, modify and communicate information. It includes the internet, but also the other information systems that support our businesses, infrastructure and services.

Incidents reported would be of a serious enough nature to require investigation.

These types of incidents could include:

- Denial of Service attacks (purposefully targeting a service with the intention of denying its users access)
- Disclosing information on Social Media
- Web site defacement
- Malicious Internal damage
- Spoof website
- Cyber Bullying

1.4.2. Suspected incidents and near misses

Initial information about an incident is often sparse and it may be uncertain whether an actual incident has taken place. **Suspected incidents and near misses should always be reported** as lessons can often be learnt from them.

In the majority of cases, the only difference between an actual and suspected incident should be whether the incident is known to have happened or MAY have happened, e.g. "I think I may have a virus on my Laptop".

A near miss is where something happened (or may have happened) but no damage occurred, e.g. virus detected by the Anti-Virus software and quarantined; a confidential letter sent to wrong address but returned unopened; a sensitive email sent to the wrong person but the recipient immediately deleted it and reported it back to the sender.

All staff (regardless of their place of work) that carries out work within or on the behalf of NHSI have a duty to report actual, suspected or near miss incidents. This will allow suspected incidents to be investigated and lessons learned.

1.5. Reporting incidents

1.5.1. Initial Reporting

All IG and cyber security related incidents should be reported, in the first instance, to the Information Governance Team. Incidents can be logged by emailing NHSI.ig@nhs.net.

This will enable the incidents to be logged, investigated, acted on and escalated as appropriate.

1.5.2. Assessing the Severity of the Incident

The immediate response to the incident and the escalation process for reporting and investigating this will vary according to the severity of the incident.

Risk assessment methods commonly categorise incidents according to the likely consequences, with the most serious being categorised as a 5, an incident should be categorised at the highest level that applies when considering the characteristics and risks of the incident. (Risk scoring card can be found at Appendix A).

1.5.3. Escalation

Minor IT incidents of an operational nature may, at the discretion of the SIRO or Deputy SIRO, be dealt with by NHSI staff in accordance with its policies and procedures. These will be summarised in a monthly report to the Information Governance Group (IGG) but need not be escalated.

If the incident is more serious or deemed to be a breach of policy, security, legislation or meets the definition of a SIRI, this must be reported immediately to the Information Governance Team who will report to the Caldicott Guardian and the SIRO.

The member of staff reporting the incident should also inform their line manager, who will assist in determining what action is appropriate and who needs to be informed and consulted.

In considering the action to be taken, the following people should be informed or consulted as appropriate:

- **SIRO/Deputy SIRO/Caldicott Guardian** – any information security incident that represents a risk to the organisation and any Serious Untoward Incident in relation to PID
- **Information Asset Owner** – any incident relating to their information assets and any incident that poses a risk to their assets, including loss of personal identifiable data
- **Director of Communications** – any incident that might result in media interest and any Serious Untoward Incident in relation to PID

On occasions, it may be necessary for incidents to be brought to the attention of external authorities:

- Information Commissioner, the Counter Fraud and Security Management Service and the Department of Health for any Serious Incident Requiring investigation at Level 3 or above
- In some circumstances, it may be necessary to inform other agencies (e.g. the Police).

Staff must not contact external authorities direct; all contact with external authorities will be through the SIRO/Deputy SIRO/Caldicott Guardian, working in conjunction with the Director of Communications.

2. HANDLING OF INFORMATION GOVERNANCE AND CYBER SECURITY SERIOUS INCIDENTS REQUIRING INVESTIGATION

2.1. Logging and Assessing Incidents

- Date, time and location of the incident
- Who discovered the incident
- Description of what happened:
  - Theft, accidental loss, inappropriate disclosure, procedural failure, etc.
  - The number of patients/ staff (individual data subjects) involved
  - The number of records involved
  - The media (paper, electronic) of the records
  - If electronic media, whether encrypted or not
  - The type of record or data involved and sensitivity

- Whether the SIRI is in the public domain
- Whether the media (press, etc.) are involved or there is a potential for media
- Interest Initial assessment of level of SIRI
- Who the incident has been reported to (e.g. Information Commissioner, Police, NHS Counter Fraud, Department of Health)
- What action has been taken to date, including any disciplinary action

As more information becomes available, the incident level should be continually re assessed to ensure that the appropriate level is maintained.

2.2. Managing the incident

Once an incident has been reported, a decision about how the case is managed needs to be made. In making that decision, the following points should be considered as appropriate:

- The SIRO/Deputy SIRO, in association with other key staff (Caldicott Guardian, Information Asset Owner, Information Governance, IT) will identify who is responsible for managing the incident
- The Director in the area where the incident occurred, in liaison with others as above will identify who is responsible for investigating and performance managing the incident
- In liaison with the Communications Team, develop and implement an communications plan
- Preserve evidence
- Investigate the incident
- Prepare formal documentation – this must incorporate version control and configuration management
- Maintain an audit trail of events and evidence supporting decisions taken during the incident
- Where appropriate, inform NHS Digital and Information Commissioner etc
- Inform data subjects
- Invoke the disciplinary procedure as necessary
- Initiate recovery actions
- Initiate appropriate counter-measures to prevent recurrence

2.3. Investigating the incident

The purpose of an investigation is not to set out to find someone to blame, it is to learn and improve. All incidents should be investigated in order to establish facts and any remedial action required.

The investigation is intended to:

- Find out all the facts regarding the sequence of events that led up to the incident
- Determine what was managed well
- Determine what (if anything) went wrong and identify any issues of concern
- Identify the ‘root causes’ that led or contributed to the incident occurring
- Make recommendations to address the root causes identified
- Identify risks and issues that, whilst not ‘in scope’ of the incident, are appropriate for separate follow-up and action
- Identify lessons learnt

2.4. Final reporting and closure of the incident

In bringing the case to a close, the following points need to be considered:

- Set target timescale for completing investigation (<5 days) and
- Produce a report (<15 days)
- Arrange for the report to be reviewed by appropriate persons or appraisal group
- Seek sign-off of the report from the Investigating Officer and SIRO/Deputy SIRO if serious enough
- Send the report to the relevant persons and/or committee (Information Governance Group, Executive Committee, etc.)
- Identify who is responsible for disseminating any lessons learnt
- Closure of SIRI
- Where the SIRI has been escalated to NHS Digital and Information Commissioner etc, notify them of the closure
- Incidents should be used to learn lessons and raise staff awareness about security and confidentiality.

Appendix A

NHSI IG shall use the following system of risk scoring:

Score	Severity of impact	Example of breach
1	Damage to an individual's reputation Possible media interest	Potentially serious breach. Less than 5 people affected or risk assessed as low
2	Damage to a team's reputation Some local media interest that may not go public	Serious potential breach and risk assessed high, e.g. unencrypted personal records lost. Up to 20 people affected
3	Damage to a services reputation Low key local media coverage	Serious breach of confidentiality, e.g. up to 100 people affected
4	Damage to an organisation's reputation Local media coverage	Serious breach with either particular sensitivity, e.g. sensitive personal records, or up to 1,000 people affected
5	Damage to organisational reputation/ National media coverage	Serious breach with potential for ID theft or over 1,000 people affected

Annex A

Reporting and Managing Incidents Diagram