PHI Public Health Institute
LIVERPOOL JOHN MOORES UNIVERSITY

DPA05
Information Incident Reporting Policy

For all staff at

PUBLIC HEALTH INSTITUTE,
LIVERPOOL JOHN MOORES UNIVERSITY

Document Reference:	DPA05
Author:	Geoff Webb
Version.Issue:	0.1
Status:	Approved
Approved by:	Dave Seddon
Version date:	November 2017
Review date:	November 2018

Approval and Authorisation

Completion of the following detail signifies the review and approval of this document, as minuted in the Senior Management Group meeting(s) shown.

Version	Authorising Group	Name of Approver	date
1.0	DPA Compliance Group	Dave Seddon	22/10/13
1.0	DPA Compliance Group	Dave Seddon	30/10/14
1.0	DPA Compliance Group	Dave Seddon	02/11/15
1.1	DPA Compliance Group	Dave Seddon	22/11/16
1.1	DPA Compliance Group	Dave Seddon	06/11/17

Document change history

Version	Status	Reason for change	date	Author
0.1	Draft	New procedure based on NWPHO document	04/06/2013	Geoff Webb
1.1	Full	changed CPH to PHI	22/11/2016	Mark Whitfield

Contents

Approval and Authorisation **2**
Document change history **2**
1. Policy Statement **4**
2. Purpose **4**
3. Scope **5**
4. Incident Types **5**
5. Roles and Responsibilities **6**
5.1 Director 6
5.2 SIRO 7
5.3 Data Guardian 7
5.4 IT Support Manager 7
5.5 Line Managers 7
5.6 All Staff 7
6. Legal and Professional Obligations **7**
7. Risk Management **8**
7.1 Objective 8
7.2 Methodology 8
7.3 Reporting 8
8. Monitoring this Procedure **8**
9. Review of this Policy **8**

1. Policy Statement

The Public Health Institute (PHI) is committed to improving the security and confidentiality of patient information and of promoting employee safety by analysing and learning from errors and adverse occurrences. The organisation is committed to developing a culture which promotes openness and honesty that focuses on improving practice, not on deficiencies and blame.

The PHI's documented and implemented processes and procedures provide a consistent approach in the handling of patient information, systems and services, which take into account the guidance, recommendations and obligations of the following:

- Care in confidentiality of Person Identifiable Data (PID)
- Consent to disclosure of PID
- Information Quality Assurance
- Information Security Management recommendations of ISO/IEC 27001:2005
- Common law duty of confidentiality
- Data Protection Act 1998
- Records Management
- Freedom of Information Act 2000
- HCC Audit

The PHI will follow a supportive and just approach in relation to incident reporting and disciplinary matters. Rather than seeking to assign blame the emphasis will be that the occurrence of an incident or an error, however serious the outcome is not in itself evidence of neglect, carelessness or dereliction of duty. Disciplinary action will only be considered in relation to any individual member of staff if evidence emerges of breaking the law, repeated poor performance that breaches professional standards of conduct, or incidents occurring as a result of reckless behaviour and gross negligence.

The PHI will report incidents to the appropriate internal management structure and, when necessary to external organisations, and will act in accordance with applicable legislation.

Incidents will be managed so that the outcomes of such events provide a framework for learning. Practice and procedures will change as appropriate in the light of lessons learned so that the chance of recurrence is reduced. The DPA group is ultimately accountable for information incidents within the organisation and will receive reports from the Deputy Director, Head of IT or Business Manager. These members of the senior management team will ensure that procedures are developed and, where necessary, reviewed and changed.

2. Purpose

Incident reporting is a primary tool of risk management, without which the latter would not be effective. An incident can generally be described as an event which has, or could lead to, a breach of information security, legislation or regulation, financial loss due to theft for example, loss of organisation reputation, or an event that has or could cause potential harm to employees. It also embraces the day to day operational problems encountered by users such as faults, lockouts and equipment malfunction. This policy covers the reporting of all such incidents.

The policy also covers the reporting of a **Near Miss** which is defined as ‘any unexpected or unintended incident which was prevented or ran to completion but did not result in an adverse outcome’.

The PHI has a duty to inform certain external agencies of specific types of incidents, e.g. the Health and Safety Executive (HSE) and Reporting of Incidents, Diseases and Dangerous Occurrences Regulations 1995 (RIDDOR).

This policy outlines procedures to follow when identifying an incident. All incidents **MUST** be reported and graded according to their severity as per the guidance within this document.

The policy applies to all permanent, temporary and contracted staff employed within the PHI, and also applies to volunteers, visitors and members of the public wishing to report an incident.

The aim of this policy is to:

- Set a framework for the proper and proactive management of incidents and thereby minimise the risk associated with them as part of the PHI’s Risk Management programme
- Ensure that the PHI meets statutory and mandatory obligations regarding the reporting of incidents

3. Scope

Confidentiality of Person Identifiable Data (PID) is required as defined in the PHI’s Confidentiality Code of Conduct. The security of that information is defined in the Information Security Management Policy. Those documents fully describe the all-encompassing scope of security and confidentiality covered by this policy.

4. Incident Types

Incident type can generally be categorised as one of the following:

- **Operational Incident** - day to day operational issues, such as user lockouts and password failures, which may be channelled through the IT Helpdesk

- **Policy Incident** – representing any failure to comply with the PHI’s Policies and any associated or supporting procedures and standards

- **Security Incident** – falling into one of three categories, namely:

  - Confidentiality – that is, incidents relating to the accidental or intentional leakage or disclosure of confidential or patient identifiable information, passwords and similar sensitive information to unauthorised persons or organisations

  - Integrity – that is, accidental or intentional damage to or inaccuracies in data

  - Availability – that is, accidental or deliberate, disruption or absence of information and services i.e. systems being down, loss of computer connections and so on

- **Fire incident -** any incident, no matter how small, involving fire or fire warning systems (including false alarms)

- **Personal Accident or Ill Health Incident -** an event that results in personal injury or any case of known or suspected work or environment related ill health, e.g. infection. This does not include any injury caused deliberately, e.g. by an act of violence or by fire

- **Complaint / Litigation Incident -** any formal verbal or written communication from any person or organisation, and in particular an incident which may lead to publicity, litigation or loss of public confidence

- **Adverse Publicity Incident –** an event that generates local media interest which could potentially pose a threat of adverse publicity

- **Financial Incident –** an event which leads to financial loss to the organisation, covering theft of assets, fraud and breaches of contracts

- **Violence, abuse or harassment –** physical and non-physical assault. This includes any anti-social behaviour, verbal abuse, bullying, abuse or harassment by reason of a person's ethnic group, religion, political opinion, age, gender, marital status, sexual orientation or disability

- **Information output -** incorrect data or information is released from PHI to an external stakeholder or the public domain

5. Roles and Responsibilities

5.1 Director

The Director has overall responsibility for the provision of security and confidentiality of information within the PHI. This responsibility is discharged through the Systems Development Manager who has specific lead responsibility for IT management (planning or operational) within the PHI.

5.2 SIRO

The PHI's Senior Information Risk Owner (SIRO) is responsible for understanding how the strategic business goals of the PHI may be impacted by information risks and for the ongoing development and day-to-day management of the PHI's Risk Management Programme for information privacy and security.

The SIRO will review and agree action in respect of identified information risks, ensure that the PHI's approach to information risk is effective in terms of resource, commitment and execution and that this is communicated to all staff.

The SIRO will provide a focal point for the resolution and/or discussion of information risk issues and ensure the Board is adequately briefed on information risks.

5.3 Data Guardian

The PHI's Data Guardian has a particular responsibility for reflecting patients' interests regarding the use of Person Identifiable Data. They are responsible for ensuring Person Identifiable Data is stored and shared in an appropriate and secure manner.

5.4 Systems Development Manager

- should ensure all current and future IT Support staff are instructed in the processes in place for the security and confidentiality of information

5.5 Line Managers

- Must ensure all current and future staff are instructed in the arrangements for the security and confidentiality of information

5.6 All Staff

- each employed, contracted and voluntary staff member is personally responsible for ensuring that procedures for security and confidentiality of information are followed

6. Legal and Professional Obligations

The PHI will take actions as necessary to comply with its legal and professional obligations.

The key statutory requirement for compliance with Information Security Management principles, is the Data Protection Act 1998 and in particular its seventh principle: *"Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of or damage to personal data".*

The PHI has legal obligations to maintain security and confidentially, in particular in accordance with the following:

Data Protection Act (1998)

Copyright Patents and Designs Act (1988)
Computer Misuse Act (1990)
Public Records Act 1958
Freedom of Information Act (2000)
Common Law Duty of Confidentiality
NHS Confidentiality Code of Practice
Any new legislation affecting records management as it arises

7. Risk Management

7.1 Objective

To identify and counter possible threats to the operation of the PHI, including the supply of IT services, through equipment failure for example, in the event of lack of maintenance.

7.2 Methodology

All systems will be subject to periodic security reviews by system managers and conducted with reference to NHS ISO 17799.

The reviews must follow the guidance in the PHI‘s Corporate Risk Assessment Policy.

7.3 Reporting

Each review will include a formal report to the PHI’s management containing findings and recommendations.

8. Monitoring this Procedure

The DPA group will monitor the implementation of this, and any subsequent revisions, as part of the annual Assessment during collection of evidence that the correct actions have been carried out.

9. Review of this Policy

This Policy should be subject to review when any of the following conditions are met:

- The adoption of the Policy highlights errors or omissions in its content
- Where other policies/strategies/guidance issued by the PHI conflict with the information contained herein
- Where the procedural or guidance framework evolves/changes such that revision would bring about improvement
- 1 year elapses after approval of the current version.