Northern Ireland Ambulance Service
Health and Social Care Trust

1.0 **Title:**	**INFORMATION RISK POLICY**		
2.0 **Author(s)**	Alison Vitty, Corporate Manager		
3.0 **Ownership:**	Finance and ICT Directorate		
4.0 **Date of SEMT Approval:**	16/03/2016 to Information Governance Steering Group	5.0 **Date of Trust Board Approval:**	07/04/2016
6.0 **Operational Date:**	10/04/2016	7.0 **Review Date:**	
Version No:	Version 1.0	**Supersedes:**	No policy to supersede
8.0 **Key words:**	Information Risk Management		
9.0 **Other Relevant Policies:**	- Risk Management Strategy - Untoward Incident Reporting Procedure - Information Governance Strategy 2015-2018 - Records Management Strategy 2015-2020 - Records Management Policy - Freedom of Information Act 2000 and Environmental Information Regulations 2004 - Data Protection Act 1998 Policy Statement - Code of Practice on the Confidentiality of Service User Information - Email Policy - Password Policy		

Version Control for Drafts:			
Date	**Version**	**Author**	**Comments**
November 15	v0.1	AV	Initial draft.
February 16	V0.1.1	AV	Further updated by Corporate Manager
16/03/2016	V0.1.1	AV	To Information Governance Steering Group. Noted. To be placed on next Trust Board
10/04/2016	V 1	AV	Placed on internet

1.0 **Introduction**

1.1 The Trust Board has approved the introduction and embedding of information risk management into the key controls and approval processes of all major business processes and functions of the Northern Ireland Ambulance Service Health and Social Care Trust (the Trust). This decision reflects the high level of importance placed upon minimising information risk and safeguarding the interests of patients, staff and the Trust itself.

1.2 Information risk is inherent in all administrative and business activities and everyone working for or on behalf of the Trust continuously manages information risk. The Board recognises that the aim of information risk management is not to eliminate risk, but rather to provide the structural means to identify, prioritise and manage the risks involved in all Trust activities. It requires a balance between the cost of managing and treating information risks with the anticipated benefits that will be derived.

1.3 The Data Handling Review by the Office of the First Minister in 2008 described the following actions to protect information and significantly mitigate risk:

- To develop relevant policies and procedures to ensure that staff are aware of the proper use of information, including at the planning stage of any project which involves person identifiable information through Privacy Impact Assessments and when services are being delivered
- To introduce obligatory use of protective measures including encryption and penetration testing and controls – these will protect personal data while recognising that some data require a greater degree of protection than others
- Mandatory training for those with access to protected information or involved in managing it, alongside action to make clear that any failure to apply protective measures is a serious matter potentially leading to dismissal.

1.4 The Board acknowledges that information risk management is an essential element of broader information governance and is an integral part of good management practice. The intent is to embed information risk management in a very practical way into business processes and functions. This is achieved through key approval and review processes / controls – and not to impose information risk management as an extra requirement.

1.5 This policy should be read in conjunction with the Trust's Risk Management Strategy/Untoward Incident Reporting Procedure and Information Governance Strategy which is the overriding strategic direction for the Trust in relation to information risk.

2.0 Purpose

2.1 The purpose of the Information Risk Policy is to:

- Protect the Trust, its staff and its patients from information risks where the likelihood of occurrence and the consequences are significant;
- Provide a consistent risk management framework in which information risks will be identified, considered and addressed in key approval, review and control processes;
- Encourage pro-active rather than re-active risk management;
- Provide assistance to and improve the quality of decision making throughout the Trust;
- Meet legal or statutory requirements; and
- Assist in safeguarding the Trust's information assets.

3.0 Scope

3.1 This policy is applicable to all areas of the Trust. Adherence should be included in all contracts for outsourced or shared services as responsibility remains with the Trust, even if an agent or sub-contractor processes data on our behalf. There are no exemptions.

3.2 For the purpose of this policy, "staff" is used to refer to all staff regardless of occupation, including but not restricted to permanent, temporary, agency, voluntary and students.

4.0 Accountability and Responsibility

Senior level ownership of information risk is central to achieving successful information management.

4.1 It is the responsibility of all staff, and anyone working on behalf of the Trust, to adhere to this policy.

4.2 Each Director must ensure that all staff, in their area responsibility, are aware of and adhere to this policy.

4.3 Managers are responsible for ensuring that all staff, in their area of responsibility are kept up-to-date with any changes and adhere to them.

4.4 The Senior Information Risk Officer (SIRO) is responsible for co-ordinating the development and maintenance of information management policies, procedures and standards for the Trust. The SIRO is also responsible for the ongoing development and day to day management of the information risk management process and any associated programmes of work. The SIRO shall advise the Chief Executive and the Trust Board on information risk management areas and provide periodic briefings and progress updates on any associated programmes of work.

4.5 The Information Asset Owners (IAOs) shall ensure that information risk assessments are performed on all information assets where they have been assigned 'ownership' following guidance from the SIRO on assessment method, format, content, and frequency. IAOs shall submit risk assessment results and associated mitigation plans to the SIRO for review, along with details of any assumptions or external dependencies.

Mitigation plans shall include specific actions with expected completion dates, as well as an account of residual risks.

4.6 The Information Asset Administrators (IAA) will ensure that policies and procedures are followed, recognise actual or potential security incidents, consult their IAO on incident management and ensure that information asset registers are accurate and up to date.

4.7 The Information Governance Steering Group (IGSG) is responsible for ensuring this policy is implemented, including any supporting guidance and training deemed necessary to support the implementation and for monitoring and providing Board assurance in this respect.

4.8 The Chief Executive is the accountable Officer responsible for the management of the Trust and for ensuring appropriate mechanisms are in place to minimise information risks and to safeguard the interest of patients, staff and the Trust itself. The Trust has a responsibility for ensuring that it corporately meets its legal responsibilities, and for the adoption of internal and external governance arrangements.

5.0 **Reporting and Monitoring**

5.1 The SIRO will provide the assessment method, format, content and frequency of reporting to the IAO. Please also refer to Appendix 1 - Procedure for IG Incidents and Investigations.

5.2 IAOs shall ensure that information risk assessments are performed annually on all assets they have been assigned ownership and submitted to the SIRO. The assessments must include plans, with specific action and completion dates along with details of assumptions or any external dependencies as well as an account of any residual risks.

5.3 The SIRO shall advise the IAOs and the Trust Board on information risk management reports and briefings on progress.

5.4 The SIRO will take ownership of risk assessment process for information risk including an annual information risk assessment to support and inform the statement of Internal Control.

5.5 The SIRO will review and agree actions in respect of identified information risks.

6.0 Risk Escalation and Event Reporting

6.1 The escalation and reporting process for the Trust is formalised through the Untoward Incident and risk management process and by using DATIX; the Trust incident and risk management application. Refer to Appendix A for the Guidance relating to Untoward Incident Reporting for Information Governance Incidents.

7.0 Definitions

7.1 Key definitions are:

- **Risk**
  The chance of something happening, which will have an impact upon objectives. It is measured in terms of *consequence* and *likelihood*.
- **Consequence**
  The outcome of an event or situation, expressed qualitatively or quantitatively, being a loss, injury, disadvantage or gain. There may be a range of possible outcomes associated with an event.
- **Likelihood**
  A qualitative description or synonym for probability or frequency.
- **Risk Assessment**
  The overall process of risk analysis and risk evaluation.
- **Risk Management**
  The culture, processes and structures that are directed towards the effective management of potential opportunities and adverse effects.
- **Risk Treatment**
  Selection and implementation of appropriate options for dealing with risk. Conceptually, treatment options will involve one or a combination of the following five strategies:
  - Avoid the risk
  - Reduce the likelihood of occurrence
  - Reduce the consequences of occurrence
  - Transfer the risk
  - Retain/accept the risk
- **Risk Management Process**
  The systematic application of management policies, procedures and practices to the tasks of establishing the context, identifying, analysing, evaluating, treating, monitoring and communicating risk.

7.2 The Information Risk Policy has been created to fit within the overall Trust Risk Management framework. Information risk should be managed separately from other business risks but should be considered a fundamental component of effective Health and Social Care information governance for the Trust.

8.0 Related Information

8.1 It is a core information governance objective that all information assets of the organisation are identified, that the business importance of those assets is established, that an information risk assessment is undertaken and that this is recorded on the Trust's Information Asset Register. The IAOs are responsible for ensuring this is undertaken.

8.2 Any residual information risks should be recorded, as per any other risk, in the Local Risk Register and managed as per the Trust's Risk Management process. Information risks that so warrant it will be on the Corporate Risk Register and managed as per the Trust's risk management process.

9.0 Review of Policy

9.1 The Policy will be reviewed by the Information Governance Steering Group every three years or as required in line with legislative or good practice guidance.

9.2 Monitoring of this policy will be informed by information governance trends reported along with any information governance Untoward Incidents which forms part of the risk management process.

10.0 Relevant Policies, Procedures and Guidance – Legislative Framework

The policy forms part of the Information Governance framework and should be read in conjunction with the following Trust policies and procedures (this is not an exhaustive list):

- Risk Management Strategy
- Untoward Incident Reporting Procedure
- Information Governance Strategy 2015-2018
- Information Risk Policy
- Records Management Strategy 2015-2020
- Records Management Policy
- Freedom of Information Act 2000 and Environmental Information Regulations 2004
- Data Protection Act 1998 Policy Statement
- Code of Practice on the Confidentiality of Service User Information
- Email Policy

11.0 EQUALITY STATEMENT

11.1 In line with duties under Section 75 of the Northern Ireland Act 1998; Targeting Social Need Initiative; Disability Discrimination Act 1995 and the Human Rights Act 1998, an initial screening exercise to ascertain if this policy should be subject to a full impact assessment has been carried out.

11.2 The outcome of the screening exercise for this policy is:

Major Impact	
Minor Impact	
No Impact	x
Still Being Determined	

12.0 SIGNATORIES

_____ **Date:** _____

Lead Author

_____ **Date:** _____

Lead Director

Information Governance
Directorate of Finance and ICT

Appendix 1

Guidance to Support Untoward Incidents Reporting Relating to Information Governance Incidents and Investigations

1.0 Introduction

1.1 The Northern Ireland Ambulance Service Health and Social Care Trust (the "Trust) has a responsibility to monitor all information governance related incidents that occur within the organisation that may breach security and/or confidentiality of personal information. The Trust also needs to ensure that all incidents are identified, reported and monitored.

1.2 This document provides advice for identifying, recording and monitoring information governance relations incidents.

2.0 Purpose

The aim of this guidance is to ensure that the Trust reacts appropriately to any actual or suspected security incidents relating to information systems and data including:

(a) Standardising the procedures for information governance (IG) investigations;
(b) Ensuring compliance with relevant legislation;
(c) There is a consistent approach to evaluating IG Untoward Incidents;
(d) Early reports of IG Untoward Incidents are sufficient to decide appropriate escalation, notification and communication to interested parties;
(e) Appropriate action is taken to prevent damage to patients, staff and the reputation of the HSC family;
(f) All aspects of Serious Untoward Incidents are fully explored and lessons learnt are identified and communicated;
(g) Appropriate corrective action is taken to prevent recurrence.

3.0 Risks

The Trust recognises that there are risks associated with users accessing and handling information in order to conduct official Trust business.

This procedure aims to mitigate the following risks:

(a) To reduce the impact of information security breaches by ensuing incidents are followed-up correctly;
(b) To help identify areas for improvement to decrease the risk and impact of future incidents.

4.0 Initial Reporting of Serious Untoward Incidents

An information governance incident may be defined as:

- The disclosure of confidential information to put any authorised person;
- The integrity of the system or data being put at risk
- The availability of the system or information put at risk
- An adverse impact e.g reputation of the Trust/HSC, threat to personal safety or privacy, legal obligation or penalty, financial loss, disruption of activity.

A breach of information governance can be a data protection and confidentiality issue, a registration authority incident, information security, records management either clinical or corporate, manual or electronic.

4.1 Suspected Incidents

Initial information is often sparse and it may be uncertain whether an Untoward Incident has actually taken place. Suspected incidents and "near misses" should be reported as Untoward Incidents as lessons can often be learnt from them and they can be closed when the full facts are known.

4.2 Early Notification

Where it is suspected that an IG Untoward Incident has taken place, it is good practice to informally notify key staff. These should include:

- Senior Information Risk Officer (SIRO): Director of Finance and ICT
- Caldicott Guardian/Personal Data Guardian : Medical Director
- Your lead Director
- Corporate Manager

They will take steps to notify the Chief Executive as required depending on the nature and level of the information risk identified.

4.3 Reporting Incidents

In line with the Trust's Untoward Incident Reporting Procedure, an Untoward Incident Form should be completed and used for reporting all incidents including information governance risks and should be made as soon as possible and no later than 24 hours of the incident or first becoming aware of the incident. Further information will become available as the investigation takes place.

4.4 The Risk Manager monitors all Untoward Incident Reports and will therefore be aware of all IG Untoward Incidents, although please note Point 5.2 regarding early notification. The Risk Manager will escalate the Untoward Incident Report as required depending on the level of risk identified.

4.5 As normal the Untoward Incident Report should be accurately and fully completed. It is important that a clear description of what has happened is clearly detailed, for example:

- Theft, accident loss, inappropriate disclosure, procedural failure etc
- The number of patients/staff (individual data subjects) involved;
- The number of records involved;
- The media (paper and/or electronic) records
- If electronic media, whether encrypted or not
- The type of record or data involved and sensitivity
- Whether the incident is in the public domain
- Whether the media (press etc) are involved are there is a potential for media attention;
- Whether the incident could damage the reputation of an individual, a work-team, an organisation or the HSC as a whole
- Whether there any legal implications for the Trust;
- Initial assessment level of the Untoward Incident;
- Immediate action taken, including whether any staff have been suspended pending the results of the investigation.

It is important to note that if at any time during the process described above either fraud, paedophilic images or criminal activity is suspected or confirmed then all investigations must cease and either the Trust's Counter Fraud Officer (Assistant Director of Finance and ICT) or the Trust Senior Information Risk Officer (Director of Finance and ICT) must be informed

It is important to keep as much information as possible of the incident and investigation confidential. No information should be discussed with anyone who is not directly involved with the incident.

6.0 Breaches of Confidentiality and Data Protection

6.1 In line the Trust's Risk Management Strategy and Untoward Incident Reporting procedure, all IG Untoward Incidents will be fully investigated by the Line Manager in the first instance and all details must be attached to the Untoward Incident reporting form.

6.2 All IG Untoward Incidents will be risk assessed in line with the Trust's Untoward Incident Reporting Policy and assessed to identify the gravity of incident and the risk to the organisation.

6.3 The Risk Manager will copy the Corporate Manager into all incidents relating to IG incidents pertaining to confidentiality and Data Protection. All incidents will be reviewed by the Corporate Manager as the Trust's Information Governance lead to ensure that the threat has been addressed or mitigated to a satisfactory level by containment activities; where required, an agreed corrective action plan had been defined and agreed that prevents reoccurrence of the vulnerability.

Information Governance
Directorate of Finance and ICT

What is an Information Governance Related Incident – Examples

1. An information governance related incident relates to breaches of security and/or the confidentiality of personal information which could be anything from users of computer systems sharing passwords, to a piece of paper identifying a patient being found in the high street.

2. An information security incident is defined as any event that has resulted or could result in:

    - The integrity of an information system or data being put at risk;
    - The availability of an information system or information being put at risk;
    - An adverse impact e.g.

        - Embarrassment to the HSC Family
        - Threat to personal safety or privacy
        - Legal obligation or penalty
        - Financial loss
        - Disruption of activities

Examples of Information Security Incidents that should be Reported:

Some more common areas are listed below but this list is not exhaustive and should be used as guidance only. If there is any doubt as to what you have found being an incident it is best to report it to the relevant personnel for their decision.

- Loss of computer equipment due to crime or an individual's carelessness
- Loss of computer media e.g. USB Stick, Compact Disc due to crime or an individual's carelessness
- Accessing any part of a database using someone else's authorisation either fraudulently or by accident
- Trying to access a secure part of the organisation using someone else's PIN number
- Finding the doors and/or windows have been broken and forced entry gained to a secure room/building
- Finding a computer printout with a header and a persons information on it at a location outside of any Trust premises/building
- Finding any paper records about a patient/member of staff or business of the organisation in any location outside of Trust premises/buildings e.g Patient Report Forms
- Being able to view patient records in an employees car
- Discussing patient or staff personal information with someone else in an open area where the conversation can be overheard
- A fax being received by the incorrect recipient
- Viewing or downloading inappropriate material
- Attempted or actual fraud

- Giving information to someone who should not have access to it – verbally, in writing or electronically
- Sending a “sensitive” email to all staff by mistake
- Use of unapproved or unlicensed software on Trust equipment
- Printing or copying confidential information and not storing it correctly or confidentiality
- Theft or loss of a hard copy file