Northern Ireland Ambulance Service
Health and Social Care Trust

1.0 Title:	INFORMATION GOVERNANCE STRATEGY 2015-2019		
2.0 Author(s)	Alison Vitty, Corporate Manager		
3.0 Ownership:	Finance and ICT Directorate		
4.0 Date of SEMT Approval:		**5.0 Date of Trust Board Approval:**	07/04/2016
6.0 Operational Date:	April 2016	**7.0 Review Date:**	September 2017
Version No:	Version 0.1.5	**Supersedes:**	Not applicable
8.0 Key words:	Information Governance		
9.0 Other Relevant Policies:	- Information Governance Policy - Information Risk Management Policy - Records Management Policy - Freedom of Information and Environmental Information Regulations Policy - General Data Protection Regulation/Data Protection Policy - General Data Protection Regulation/Data Protection Manual		

Version Control for Drafts:			
Date	**Version**	**Author**	**Comments**
	V0.1.1	AV	Initial draft.
	V0.1.2	AV	Further updated – June 2015
	V0.1.3	AV	Further updated – August 2015
	V0.1.4	AV	Minor amendments made based on comments from Senior Information Risk Owner and Personal Data Guardian/Caldicott Guardian
	V0.1.5	AV	Minor amendments from SEMT – March 2016
	V0.1.6	AV	Amendments due to replacement of Data Protection Act 1998 by General Data Protection Regulation/Data Protection Act 2018 – May 2018.

1.0 **Executive Summary**

This Strategy contains the Northern Ireland Ambulance Service HSC Trust information governance aims and deliverable programme for 2015-2019.

The Information Governance Assurance Framework (IGAF) is a national framework of standards that bring together all statutory, mandatory and best practice requirements concerning information management. The standards are set out in the Information Governance Control Assurance template as a road map enabling NIAS to plan and implement standards of practice and to measure and report compliance on an annual basis.

It confirms fully the Trust's commitment to compliance with information rights and legislative requirements.

It aims to set out an approach that will deliver all of the essential compliance elements, in a way that also enables and supports the delivery of corporate objectives and opportunities for organisational benefits. It is an approach that will be flexible and responsive to new or changed operational and legislative requirements and that will enable the Trust to take proportionate risk.

It demonstrates how effective information governance can help the Trust to make the best use of information, and as a consequence, assist in the delivery of our objectives and the improvement of our day to day processes.

It is an approach which will enhance our corporate objectives to be open and transparent about what we do, and to be held to account for the actions we take. It will give confidence to those who provide their personal information to us whether they are staff, patients or stakeholders that their information will be managed appropriately and securely.

We will ensure that we communicate and champion the Information Governance Strategy and information governance agenda throughout the Trust and wider public domain. Information plays a key part in all Directorate areas within Trust. The quality in the provision of services planning, performance measurement, assurance and financial management relies upon accurate, timely and available information.

Information is a key asset to the Trust and Information Governance is a corporate-wide agenda that will not succeed if it is seen in isolation from the integrated Corporate Assurance agenda and it should therefore be afforded appropriate authority.

The document sets an overarching framework for the strategic Information Governance agenda within NIAS.

2.0 INTRODUCTION

This strategy describes the continuing development, implementation and embedding of a robust information governance framework needed for the effective management and protection of the Trust's information.

Information governance describes the approach within which accountability, standards, policies and procedures are developed and implemented, to ensure that all information created, obtained or received by the Trust is held appropriately.

The Trust relies on good accurate quality information being available at the point of need in order to provide a quality service. Staffs need to have confidence in the quality of data they use to make decisions about patient care and treatment and the way in which we use resources and run our day to day business. All staff should understand their own responsibility for recording information to a consistently high manner and for keeping it secure and confidential. Public confidence in our ability to handle their data responsibly and efficiently is based on a good reputation for keeping their data safe and from their own personal experience when using our services.

The importance of IG was highlighted during 2008 when public concerns about high-profile data losses and protection of privacy were reported in the media and a range of standards and processes were developed for managing information risks and were subsequently mandated and incorporated into the DHSSPS Information Management Controls Assurance Standard.

The associated NHS review led to the existing IG agenda being strengthened to become an Information Governance Assurance Framework (IGAF). IGAF is formed by elements of statue and policy from which information governance standards are derived, and the activities and roles which individually and collectively ensure that those standards are clearly defined and met.

A particular feature of the IGAF was to introduce a framework of accountability for information risk with the mandated appointment of a Board level Senior Information Risk Owner (SIRO) who takes responsibility for managing information risk within the Trust and for providing assurance to the Accountable Officer on the content of the annual Statement of Internal Control in regards to IG.

At a local level, the framework enables the Trust to set annual objectives to achieve the required standards and to report organisational performance measures and assurance of compliance to Internal Audit and to the general public.

This document should be read fully in conjunction with the Information Governance Policy and other associated policies and procedures detailed in the cover sheet of the document.

3.0 Regulatory Environment

The IGAF is an encompassing term for a number of different areas. It brings together all legal requirements, standards and best practice guidance that apply to the handling and use of information and information assets. It is primarily driven by statues including but not limited to:

- Data Protection Act 1998 (replaced in May 2018 by the General Data Protection Regulation (GDPR) and Data Protection Act 2018
- Freedom of Information Act 2000
- Access to Health Records (NI) Order 1993
- The Environmental Information Regulations (NI) 1992
- Privacy and Electronic Communications Regulations 2003
- The Public Records Act 1958
- Disposal of Documents Order 1925
- The Re-Use of Public Section Information Regulations 2005
- Computer Misuse Act 1990
- The Common Law Duty of Confidentiality
- The Human Rights Act 1998
- Electronic Communications Act 2000
- The Regulation of Investigatory Powers Act 1995
- BS ISO/IEC 27001:2005; ISO/IEC 27001:2013.
- ISO/IED 27001.
- DHSSPSNI Code of Practice on Protecting the Confidentiality of Service User Information 2012.
- The Personal Data Guardian Manual 2012.
- Information security assurance
- Information quality assurance.
- Records Management
- The ICO's published guidance and Codes of Practice

4.0 Annual Information Management Assurance

The Annual Information Management Assurance is measured via an assessment process of compliance against the standards set out in the DHSSPSNI Controls Assurance Standard on Information Management.

If any gaps in compliance are identified an action plan will be produced to recover, improve or maintain the required performance levels. Through the development and routine reporting of agreed key performance indicators, identify risks, measure progress, oversee necessary remedial action is taken to ensure compliance.

However, this Strategy establishes the overall direction of IG and the baseline principles and objectives so that it will endure.

Please note that from 2018/19 the Controls Assurance standard has been redefined and assurance is given via a completed return rather than previous process of all areas being audited and evidence reviewed.

5.0 Statement of Compliance

The Trust will comply with all standards as laid out in the Information Management Control Assurance Standard and will seek to maintain substantive compliance on a yearly basis.

6.0 Information Governance Aims

The Trust's information governance aims are outlined below. Deliverables to support the achievement of these aims are described under Section 8.0 below. Achievement of these aims will deliver essential compliance elements but will also enable and support our organisation and deliver organisational benefits.

6.1 Policy

We will implement information governance policies and procedures which are embedded in the day to day operation of the Trust and which are compliant with relevant legislation, Standards and Codes of Practice and demonstrate good practice.

We will implement risk based information governance policies which are clear, accessible, and flexible and aligned with business requirements.

6.2 Awareness

We will ensure that the information governance assurance framework has a high level of awareness through the development and communication of policies, appointment of specific information governance roles across the Trust and develop processes to help achieve compliance and reduce the risk of non-compliance through human error. Please refer to the Trust's Information Policy for all IG roles appointed within the Trust.

We will foster a culture of personal responsibility, ownership and commitment to high standards in information handling to support and enable our organisational processes.

6.3 Monitoring and Assurance

We will ensure that there are processes in place to check that the information governance framework is being implemented and to measure the effectiveness of the control environment.

We will work across Directorate areas and with Information Asset Owners prompting feedback about the practical operation of policies and procedures to maximise the opportunity to learn from example of good practice.

The Trust's IG performance will be measured through the self-assessed baseline, improvement and annual IG Controls Assurance Standard and reported to the IGSG and DHSSPS. The Control Assurance Standard for Information Management sets the requirement for all HSC organisations to achieve substantive compliance against all relevant key criterions which is set at 75% and above. There are a total of 27 criterions for the IG Controls Assurance Standard with sub-criterions within each.

The Trust will develop key performance measures to monitor progress and highlight gaps, which are reportable to the Trust Board via the Assurance Committee.

Performance will also be measured and monitored through a programme of internal audit.

The NIAS Information Governance Steering Group (IGSG) will be responsible for challenging the performance report and ensuring actions are taken to address shortfalls.

The IGSG Chair (Director of Finance and ICT) will report the Trust's IG performance to the Assurance Committee and then to Trust Board.

6.4 **Records and Information Management**

We will ensure that effective processes are in place to manage our records and information. From creation, to receipt or through to disposal we will aim to meet our obligations under the records management agenda and Public Records Act and the records management guidance set out under Section 46 of the Freedom of Information Act 2000.

The integrity of information will be assured, monitored and maintained to ensure that it is of quality and reliable for use for the purposes that it is collected for.

6.5 **Information Security**

We will implement information security policies and procedures which take account of legislative requirements and codes of practice which we are subject to but which are proportionate, measured and part of Trust business as usual.

We will support our staff by ensuring that information security protocols and processes are clear and accessible, that help and guidance are available when needed and by providing appropriate training to minimise the risk of human error.

6.6 **Collection and Use of Personal Information**

Personal information received or obtained by the Trust will be managed and used responsibly, securely and fairly.

Information will be organised and managed in accordance with mandated and statutory standards and kept confidential where appropriate.

We will promote transparency and openness about how we handle personal information providing confidence to staff, service users and third parties who pass personal information to us.

The Trust will protect personal data held in its information systems through compliance with ICT Controls Assurance Standard, ICT Strategy and associated good practice standard of ISO/IEC 27002:2005.

The Trust will ensure that its Data Protection notification is reviewed and updated annually and accurately reports all processing of personal data within the organisation.

The Trust, as the legal person, will ensure that its personal data is controlled and managed in accordance with the terms of the Data Protection Act 1998 principles. *From May 2018 in line with the General Data Protection Regulations/Data Protection Act 2018. A Data Protection Officer has also been appointed within the Trust.*

6.7 **The Trust will ensure that adequate governance arrangements and resources are in place to support the IGAF agenda**

The general purpose of the IG Strategy is set out the Trust's approach to IG. It aims to promote a culture of good practice around processing and management of information and the use of information systems throughout the Trust.

The IG Strategy cannot be viewed in isolation as information is central to all area of work within the Trust.

IG is also a key element of corporate, clinical and risk governance. This strategy is therefore closely linked with other Strategies and Policies to ensure integration with all aspects of the Trust's daily activities e.g Communications Strategy, ICT Strategy etc

The Trust will ensure that adequate governance resources are in place to support the current and evolving IGAF agenda. This will be achieved through compliance with the Information Governance Management Assurance standards.

The Trust's Information Governance Steering Group will be responsible for steering the Trust's IG Agenda (see Appendix A).

6.8 **The Trust will ensure patients and the public are effectively informed and know how to access their information and exercise their right of choice**

The Trust will develop and maintain a Communications Strategy to ensure that patients, stakeholders and the public are adequately informed about confidentiality and the way their information is used and shared, their rights as data subjects, in particular how they may access their personal data and how they may exercise those rights when consent is required to use their data for non-clinical purposes. Effective procedures will be introduced to address that detailed questions raised by patients and aim for their right of choice can to be exercised and respected. Privacy notices for both staff and the public have also been created so that individuals clearly know what information we are collecting and processing on their behalf.

6.9 **The Trust will provide assurance that all information risks are identified, managed and mitigated**

The Trust will establish clear lines of accountability for information risk management that lead directly to the Board through the appointment of a Senior Information Risk Owner (SIRO), IAOs (Information Asset Owners) and the development and maintenance of an Information Asset Register.

The SIRO (via IAOs) will report to the Accountable Officer for the management and mitigation of information risks and will provide assurance to that effect for the Annual Report and Statement of Internal Control.

7.0 Strategy Review

This Strategy establishes the overall direction of IG and the baseline deliverables and programme of work over the following years so that it will endure. The review period for this strategy has therefore been established at the tolerated maximum of three years.

The Annual Plan however will need to be refreshed and reviewed on an annual basis to monitor deliverables. The IGSG will ensure this strategy is reviewed on an annual basis along with associated Action Plans relating to IG management under the remit of the Controls Assurance Standard and/or Internal Audit Recommendations.

8.0 EQUALITY STATEMENT

8.1 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.

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

Major Impact	
Minor Impact	
No Impact	
Still Being Determined	X

9.0 SIGNATORIES

_____ **Date:** _____

Lead Author

_____ **Date:** _____

Lead Director

INFORMATION GOVERNANCE DELIVERABLES/IMPROVEMENT PLANS

The deliverables to support the achievement of the Trust's information governance aims over the next three years are detailed below. This includes deliverable action points, including resource implications and timescales for completion. Resources noted as Business as Usual (BSU) are covered by current job descriptions but may need fresh impetus or action.

12.1 Maintain Policy and Procedures and keep the Trust Board Informed

Deliverable	Delivering Compliance	Action Point	Lead	Timescale	Review Mechanism	Resource Implication	Benefit
A review of all information governance policies to include development of new policies and procedures as required	Policies which achieve legal compliance, demonstrate good practice and are in line with legislative requirement	Review IG framework Policies including (this is not an exhaustive list): Data Protection Policy Data Protection Manual 2013 Data Quality Policy Records Management Strategy Records Management Policy Freedom of Information Policy Freedom of Information Procedure Information Sheets ICT Strategy Email Policy Password Policy	Corporate Manager	March 2016 Ongoing	Policy Review Report	BAU	IG Policies and supporting framework documentation remain up to date and relevant

		Develop IG Strategy	Corporate Manager	Jan 2016 Ongoing	Ongoing improvement in line with IG Controls Assurance Standard	BAU	To develop an IG culture across the Trust that can be measured against SMART objectives and deliverables
		Develop IG Policy	Corporate Manager	October 2015 Ongoing	Ongoing improvement in line with IG Controls Assurance Standard	BAU	To develop an IG culture across the Trust that can be measured against SMART objectives and deliverables
		Provide Trust Board Update, IG Strategy and IG Policy Signed Off	Director of Finance and ICT	Jan 2016 Ongoing	Trust Board Minute	BAU	The Trust Board is responsible for is responsible for ensuring that the information governance function is appropriately managed in a manner which complies with relevant legislation and standards.
		Ensure retention of adequate resources and expertise in IG related functions	Director of Finance and ICT	Ongoing		BAU	Trust as all relevant expertise covered

9.1 Awareness

Deliverable	Delivering Compliance	Action Point	Lead	Timescale	Review Mechanism	Resource Implication	Benefit
Communication and promotion of the revised information governance policies to all staff and third parties who work with the Trust	High levels of awareness to minimise risks of non-compliance through human error	Redistribute to all staff IG policies and procedures with summary of content and responsibilities to develop an IG culture through the use of the Intranet and other associated communication tools	Corporate Manager Executive Directors Information Asset Owners	Ongoing	Feedback through monitoring; staff surveys; training sessions	BAU	Policies and procedures are managed and communicated appropriately
Maintain visibility of IG Training	Monitoring of IG training will enable timely compliance with agreed Learning and Development Plans for staff. Local ownership and accountability for information governance issues and driving compliance.	Regional Ambulance Training Centre to provide quarterly reports on IG training aspects including induction and refresher training for all staff	Director of Human Resources and Corporate Services	Quarterly basis	Training provision will be audited against IG training plan and training attendance levels	Staff Resources Financial Implications	Training is vital to support staff awareness and compliance
		Agreed IG training plan for all IG roles through the Trust to be developed for all staff and specific IG roles	Director of Finance Corporate Manager	Ongoing	IG Staff Training Strategy	Staff Resources Financial Implications	Training is vital to support awareness and compliance and to foster and IG culture

		Developed and implemented training programme for Information Asset Owners (IAOs)	Director of Finance Corporate Manager	Ongoing	Training Records	Staff Resources Financial Implications	Specialised training is vital to support staff awareness and compliance
		Developed and implemented training programme for Information Asset Assistants (IAAs)	Director of Finance Corporate Manager	Ongoing	Training Records	Staff Resources Financial Implications	Specialised training is vital to support staff awareness and compliance

9.2 Monitoring and Assurance

Deliverable	Delivering Compliance	Action Point	Lead	Timescale	Review Mechanism	Resource Implication	Benefit
A developed and embedded integrated information governance framework as part of day to day business with annual assessments eg DHSSPS Controls Assurance Standards Internal Audit	A tool to provide assurance to the Trust Board, SIRO and Audit Committee to monitor compliance	Annual assessment of DHSSPS Information Governance Controls Assurance Standard Partake in IG internal audits as required	Corporate Manager IAOs Corporate Manager IAOs	Annual Ongoing	Self-Assessment compliance level Self-Assessment Compliance Levels	Staff Resources Financial Implications Staff Resources Financial Implications	Compliance with requirements. Also structured opportunity for IAOs to consider information governance compliance. An opportunity to identify and address corporate issues identified by IAOs and self-assessments
Review Content of Staff Terms of Employment to ensure that IG requirements are detailed	Appropriate organisational measures to support IG framework	Liaise with HR and Corporate Services Directorate to ensure IG content evident in staff terms of employment	Corporate Manager	March 2016	Evidence of correct clauses used	BAU	Compliance with requirements on staff contracts

A review of the pre-employment security check processes and the adoption of any recommendations	Appropriate organisational measures to support IG framework to satisfy Principle 7 under the remit of the Data Protection Act 1998/General Data Protection Regulations	Liaise with HR and Corporate Services Directorate to ensure IG content evident in staff terms of employment	Corporate Manager	March 2016	Evidence that processes are in place	BAU	Reduced risk of employing inappropriate staff potentially saving time and money
Review content of contractors terms and conditions relating to IG aspects to minimise potential breaches of confidentiality	Appropriate organisational measures to support IG framework	Liaise with relevant internal and external stakeholders e.g BSO regarding contract IG content	Corporate Manager	March 2016	Evidence of correct clauses used	Staff Resources	Compliance with requirements on contractors' contracts
Ensure correct clauses included in suppliers contracts (via Procurement)	Appropriate organisational measures to support IG framework	Liaise with relevant internal and external stakeholders e.g BSO regarding contract IG content	Corporate Manager	March 2016	Evidence of correct clauses used	Staff Resources	Compliance with requirements on procurement contracts
A review of IT processes including taking and storing IT back up media and the disposal of IT equipment and the adoption	Appropriate organisational measures to support IG framework to satisfy Principle 7 under the remit of the Data	Review of ICT Strategy and liaise with internal stakeholders ie ICT Manager	Corporate Manager IT Manager	March 2016	Evidence that processes are in place	Staff Resources	Confidence that information will be available to the Trust when required and information will be securely disposed of when no longer required

of recommendations	Protection Act 1998/General Data Protection Regulations						
Physical Security Measures are tested, validated and assured by Audit and assessments	Appropriate organisational measures to support IG framework to satisfy Principle 7 under the remit of the Data Protection Act 1998/General Data Protection Regulations	Partake in self-assessments and audits as required	Corporate Manager ICT Manager	March 2016	Evidence that processes are in place	Staff Resources Financial Implications	Reassurance to staff about their safety in the workplace, mechanisms to support the protection of personal information are evident and to minimise the risk of information security incident interrupting business continuity
Broaden Monitoring of Subject Access Requests under the remit of the Data Protection Act/General Data Protection Regulations	Appropriate monitoring of legislative requirement for Subject Access Requests	Make direct requests more efficient	Corporate Manager	Ongoing	Reports to be provided to Trust Board and associated Committee structures	Staff Resources	Improved accuracy on logging and monitoring of Subject Access Requests
		Monitor Solicitor Requests	Corporate Manager	Ongoing	Reports to be provided to Trust Board and associated Committee structures	Staff Resources	Improved accuracy and monitoring on indirect requests

		Monitor Police Service of Northern Ireland requests	Corporate Manager	Ongoing	Reports to be provided to Trust Board and associated Committee structures	Staff Resources	Improved accuracy and monitoring on indirect requests
		Monitor Coroner Service for Northern Ireland requests	Corporate Manager	Ongoing	Reports to be provided to Trust Board and associated Committee structures	Staff Resources	Improved accuracy and monitoring on indirect requests
		Corporate Manager to regularly report on all patient DPA requests ie - Social Worker Enquiries - Police Ombudsman - HSC Trust investigation	Corporate Manager	Ongoing	Reports to be provided to Trust Board and associated Committee structures	Staff Resources	Improved accuracy and monitoring on indirect requests
Audit faxes locations throughout the Trust and identify safe haven faxing requirements	Appropriate organisational measures to support IG framework to satisfy Principle 7 under the remit of the Data Protection Act 1998/General Data Protection Regulations	Information Asset Owners to take responsibility for audit of fax machines and to provide reports as required	Corporate Manager IAOs	March 2016	List on Telephone Directory	Staff Resources	Assurance that required faxes operate as safe haven and all staff are aware of same

Ensure all regular flows of data, internal and external are secure	Appropriate organisational measures to support IG framework	Information Audit and identification of information risk assets	IAOs	December 2015 (ongoing)	Information Asset Register	Staff Resources	