Information Governance Policy

Date: **December 2018**

Version: **3.05**

Author: **Stuart Hubbard, Information Manager**

Review Date: **January 2020**

If you would like this document in a different language or format, please contact Corporate Services on 01595 743064

Name of document	Information Governance Policy	
Registration Reference Number	FIPOL002	**New ☐ Review ☑**
Author	Stuart Hubbard	
Executive Lead	Colin Marsland	

Proposed groups to present document to:	
Information Governance Sub Group	
Information Support Group (ISG)	
Clinical Services Management Team (CSMT)	
Clinical Governance Committee (CGC)	

Date	**Version**	**Group**	**Reason**	**Outcome**
31st October 2012	2.0	Information Sub Group	Planned review	MR
14th November 2012	2.0	ISG		PRO
22nd January 2013	2.0	CSMT		PRO
29th January 2013	2.01	CGC	Request for approval	Approved- MR
29th May 2013	2.04	ISG	Request for approval	MR
20th Nov 2013	2.05	ISG	Request for approval	PRO
17th Jan 2017	3.01	eISG	Planned Review	MR
14th Feb 2017	3.02	CCPGC	Request for approval	MR
20th Sep 2018	3.03	eISG	Updated policy map	MR
5th Dec 2018	3.03	IGSG	FIO	MR
12th Feb 2019	3.04	CCPGC	Request for approved	Approved-MR

Examples of reasons for presenting to the group	**Examples of outcomes following meeting**
• Professional input required re: content (PI)	• Significant changes to content required – refer to Executive Lead for guidance (SC)
• Professional opinion on content (PO)	• To amend content & re-submit to group (AC&R)
• General comments/suggestions (C/S)	• For minor revisions (e.g. format/layout) – no need to re-submit to group (MR)
• For information only (FIO)	• Recommend proceeding to next stage (PRO)

*To be attached to the document under development/review and presented to the group
Please record details of any changes made to the document on the back of this form

DATE	CHANGES MADE TO DOCUMENT
22.1.13	Added section on Subject Access requests. Created version 2.01
4.2.13	Minor revisions to role of Risk Management group added.
31.5.2013	Version 2.04. IT security and Information Security policies split apart, transportation of Medical Records policy added.
20.11.2013	Web links updated to reflect new website
Dec 2016	Policy map on page 8 refreshed Former appendix A split into two appendices – here appendix A and B – for clarity Names and Job Titles in Appendix C refreshed.
Jan 2017	Sub-contractors added to scope in section 1 Risk management Group added to list of roles and responsibilities in section 11
Sep 2018	Changes made to 3.03: Added IG Breach Reporting Procedure to policy map
Dec 2018	Replaced named post holders appendix
Jan 2019	Changes made to 3.03: Replaced hyperlink to missing Knowledge Network pages in Section 4. Added intranet hyperlink to Appendix C. Removed the reference to “Draft Health Records Policy” 2016 in Section 3 and added “Access to Health Records Procedure” and Internet hyperlink.
Feb 2019	Changes made to 3.04: Corrected the information regarding the Chair of the Clinical Care and Professional Governance Committee in Section 11. Changed “Information Governance Sub Committee” to “Information Governance Sub Group” for naming consistency.

Review Date: January 2020

Table of Contents

Item	*Table of Contents*	*3*
1	*Scope of the document*	*5*
2	*Introduction*	*5*
3	*Openness*	*5*
4	*National policy aims and objectives*	*6*
5	*Local Approach to Information Governance*	*7*
6	*Subject Access Requests*	*9*
7	*Electronic Information Systems*	*9*
8	*Information Management & IG Security*	*10*
9	*Training and development*	*11*
10	*Annual IG Objectives*	*11*
11	*Roles and responsibilities of key staff*	*12*
12	*Communication*	*14*
13	*Supporting documents*	*15*
14	*Action plan – High Level*	*15*
15	*Policy Breaches*	*15*
16	*Conclusion*	*16*

Appendix A	*Information Governance organisation chart*	*17*
Appendix B	*Information Governance line management chart*	*18*
Appendix C	*List of membership of relevant standing committees*	*19*
Appendix D	*Rapid Impact Assessment for Diversity*	*20*

INFORMATION GOVERNANCE POLICY

1. SCOPE OF DOCUMENT

This policy sets out the strategic approach and objectives for providing a robust Information Governance (IG) framework for the management of information, across Shetland NHS Board (the Board).

This document applies to all directly employed staff within the Board. It is recommended as good practice guidance for all of the independent primary care contractors. Sub-contractors to NHS Shetland will be required to adhere to NHS Shetland's IG principles laid out in this policy.

This document supersedes version 2 which has been updated as part of the scheduled document review process.

2. INTRODUCTION

The Board recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. The Board fully supports the principles of corporate governance, clinical governance and information governance. The Board recognises its public accountability, but equally places importance on the confidentiality of and the security arrangements to safeguard both personal information about patients and staff and commercially sensitive information. The Board also recognises the need to share patient information with other health organisations and other agencies in a controlled manner consistent with the interests of the patient and, in some circumstances, the public interest.

The Board believes that accurate, timely and relevant information is essential to deliver the highest quality health care. As such it is the responsibility of all clinicians and managers to ensure and promote the quality of information and to actively use information in decision-making processes.

3. OPENNESS

Information will be identified and where appropriate kept confidential, underpinning the principles of Caldicott and the regulations and principles as outlined in the Data Protection Act 1998. The Patient Confidentiality policy can be found at the following link:
http://www.shb.scot.nhs.uk/board/policies/PatientConfidentiality.pdf

Patients have access to information relating to their own healthcare, options for treatment and their rights as patients. There are clear procedures and arrangements for handling queries from patients and the public. Details are described in the Access to Health Records Procedure. This document can be found at:

https://www.shb.scot.nhs.uk/board/policies/AccesstoHealthRecordsProcedure-v3.pdf

The Board has clear procedures and arrangements for liaison with the press and broadcasting media.

The Board ensures that the exchange/sharing of any information is only carried out when necessary, and within the policy parameters set between the information sharing agencies and where appropriate with the individuals consent. Details are described in the Data Sharing Policy at the following link:

http://www.shb.scot.nhs.uk/board/policies/ShetlandDataSharingPolicy.pdf

The Board regards all identifiable personal information relating to patients as confidential, except where legislation requires otherwise.

The Board has established and maintains policies and procedures to ensure compliance with the Data Protection Act, Human Rights Act, the common law duty of Confidentiality and the Freedom of Information Act.

4. NATIONAL POLICY AIMS AND OBJECTIVES

The eHealth Strategy 2011 – 17 covers the approach that the Scottish NHS takes to Information and how Information should be used to improve healthcare. This strategy was refreshed in 2014, and the refreshed document can be found at:

http://www.gov.scot/Resource/0047/00472754.pdf

Information Governance has four key aims:

- To support the provision of high quality care by promoting the effective and appropriate use of information.
- To encourage responsible staff to work closely together, preventing duplication of effort and enabling more efficient use of resources.
- To develop support arrangements and provide staff with appropriate tools and support to enable them to carry out their responsibilities to consistently high standards.
- To enable the organisation to understand its own performance and manage improvement in a systematic and effective way.

Information Governance operates within the national legal context; most importantly:

- Access to Health Records Act 1990 (where the Act still applies)
- Data Protection Act 2018
- Data Protection (Processing of Sensitive Personal Data) Order 2000
- Public Records (Scotland) Act 2011
- Computer Misuse Act 1990
- Human Rights Act 1998
- Adults with Incapacity Act 2000
- The Freedom of Information (Scotland) Act 2002
- BS799 and ISO 17799 - Information Security Standards
- Confidentiality: NHS Scotland Code of Practice on Protecting Patient Confidentiality 2003
- Records Management NHS Code of Practice 2012
- The Common Law
- Professional Guidance (e.g. from the GMC, NMC etc)

Others may be included as Information Governance develops, but a comprehensive working context is given at https://www.informationgovernance.scot.nhs.uk/ . These acts make explicit which items are confidential – principally personal information relating to patients or to staff – and where the Board is open. In all cases, information is disclosed or withheld according to the relevant procedures.

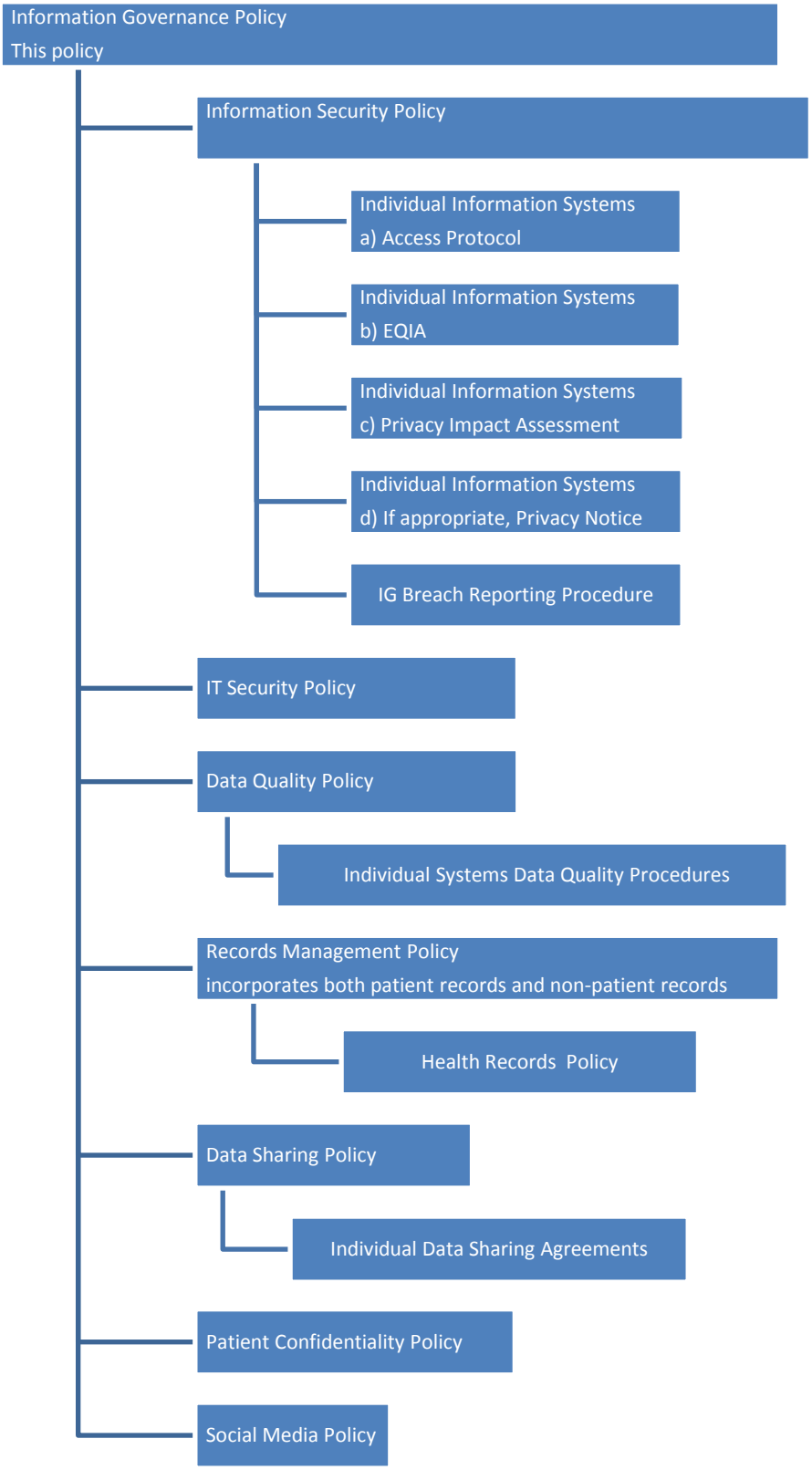
Information Governance relates to all aspects of Information in the Scottish Health Service, but by far the largest area is in relation to Patient related information. For this area, a comprehensive working context is given by Health Rights Information Scotland in their website at: http://www.gov.scot/Resource/0040/00407723.pdf

5. LOCAL APPROACH TO INFORMATION GOVERNANCE

There are two key components underpinning this policy which are:

- The Board IG Policy itself, along with its companion policies and procedures, which outline the objectives for information governance and how they are to be approached; and
- An action plan setting out objectives and deliverables against the IG national standards.

The chart below describes the relationship between the companion policies and procedures, which underpin our local IG infrastructure.



This strategy cannot be seen in isolation as information plays a key part in the delivery of clinical governance and risk management frameworks, service planning and performance management. The policy therefore links into all of these aspects of the organisation and is also reflected in the risk management strategy and the clinical governance strategy.

6. SUBJECT ACCESS REQUESTS

A subject access request is where an individual requests to see information held in an information system about themselves. This applies not only to patients, but also to staff, contractors and so on. This right is part of the provisions of the Data Protection Act. Not only may individuals make a subject access request, but if their information is shown to be incorrect there is also provision that the information be corrected. This policy recognises that standard operating procedures should cater for subject access requests, and this is dealt with in the Records Policy.

7. ELECTRONIC INFORMATION SYSTEMS

The Board runs a number of electronic information systems to assist with all aspects of its business, not only for patient care but also for staff, finance and so on. Each of these will have a set of governance documents which are tailored to the system in question. At the very least, this set must include an Access Protocol and an Equality and Diversity Impact Assessment. The Access Protocol may or may not call in addition for a Privacy Impact Assessment and/or a Privacy Notice.

For new information systems, this documentation must be in place prior to the system “going live”.

The Access Protocol describes who may use the system and for what purpose. It also covers the type of data that is in place. In general, it describes how the Board conducts itself with regard to the operation of that system. It will include a description of the audit that this required in order to assure the Board that Information Governance policy standards are maintained, and it will include a sign-off sheet which must be completed by system users before an account may be activated.

The Equality and Diversity Impact Assessment describes how use of the system may or may not affect any group differently from any other group, in particular with regard to gender, race, age, sexuality or disability.

The Privacy Impact Assessment describes how use of the system may impact any individual’s privacy, in particular with regard to the confidentiality of any details stored by the system and the way that details may be shared. Although this is of great importance to patient data, it is relevant also to any other individuals who are involved in the system.

The Privacy Notice is a public notice which may be required to alert individuals regarding details of how their information is treated and shared. Over and above patients and staff, this may also extend to members of the public and other groups of individuals.

8. INFORMATION MANAGEMENT & IG SECURITY

It is important that information held by the Board is up-to-date, accurate, accessible validated and scrutinized. In order to ensure that appropriate systems are in place for data validation, the Board will ensure that external audits will be undertaken annually to review the following IG topics:

1. Data protection
2. IT security
3. Data validation of key information systems (e.g. Patient Administration System)
4. Data validation of waiting times systems and application of national rules and definitions (e.g. access to hospital services, access to cancer services).

The Board also participates in NHS Scotland[1] facilitated data validation audits such as the national cancer audit programme, implementation of 'New Ways Rules' audit programme, implementation of recording of patient unavailability and other programmes that may arise from time to time.

There is also a local programme of audit in place to review compliance with Board policies and procedures and includes the following:

1. Validation of admission type and location
2. Application of waiting list and scheduling rules
3. Clinical Coding
4. Casenote Management (including review against the retention and destruction procedure)

In addition to this, the Board has put in place robust systems for reviewing and approving performance data (e.g. waiting times data shown in monthly management information (MMI) reports and diagnostic monthly management information (DMMIs) reports, Data warehouse submissions and other government returns).

1. National returns are validated and approved by the Chief Executive (or deputy) before submission.
2. Cancer returns are validated and approved by the Director of Clinical Services (or deputy) before submission.
3. Monthly returns showing delayed discharges are validated and approved by the Admissions and Discharges Group, which meets weekly.

Policies have been put in place to support staff to work within the IG framework. The policies include information to ensure that personal information is:

- Held securely and confidentially
- Obtained fairly and lawfully
- Recorded accurately and reliably
- Accessible when required
- Used effectively and ethically
- Shared appropriately and legally

[1] This includes audits facilitated by NHS Quality Improvement Scotland, NHS National Services Scotland, Information Statistics Division and National Clinical Networks such as the national cancer networks

The IT Security Policy, Information Security Policy and Health Records Management Policy form part of the Board's IG security arrangements. These topics are discussed at staff induction sessions and at the compulsory refresher sessions. All staff are issued national guidance on Information Governance.

IG incidents are reported to the eHealth and Information Support Group (eISG) on a quarterly basis. The eISG fulfils the role of the Board's Information Governance Committee. This includes: technical incidents (systems outage, business continuity plan failure etc), information management incidents (e.g. where validation process shows inaccuracies such as patient identification errors) and other information governance incidents such as breach of confidentiality, breach of policy, data protection act breach and loss of data incidents (e.g. via loss of mobile device etc).

Lessons learnt are cascaded to staff at all levels. Formal reporting includes an annual report on IG incidents and discussion of high-risk areas via the NHS Shetland Clinical Care and Professional Governance Committee (CCPGC).

9. TRAINING & DEVELOPMENT

Fundamental to the success of delivering the IG strategy is development of an IG culture within the Board. Awareness and training needs to be provided to all Board staff utilising the information in their day-to-day work to promote this culture. In order to achieve this; a training programme has been developed which includes key topics such as confidentiality, IT security, data sharing, data protection and privacy impact assessment. The training programme is part of the mandatory training for all staff employed by the Board. All staff are required to attend the update on an annual basis. Uptake of training is monitored through the Board's monthly performance report and eISG.

In addition to this, more detailed or specialist training is made available to staff with key IG roles to ensure they are up to date and able to carry out lead roles. This includes training built into personal development plans (PDPs) for lead officers such as the Health Records Manager, IM&T Manager and Information Manager. A training programme for medical records staff is being developed to ensure that new and existing staff are kept up to date with local policies, procedures and good practice.

10. ANNUAL IG OBJECTIVES

Each year the eHealth and Information Support Group, through its Information Governance Sub Group, will produce an annual report which will describe explicitly Information Governance objectives for the forthcoming year. The eISG will authorise specific pieces of work as appropriate, but common threads which will occur every year will include:

- Revise and maintain policies and procedures for the effective and secure management of its information assets and resources.
- Ensure that the local IG plan complies with best practice standards and national IG standards.
- The staff training programme will be enhanced to support the embedding of and implementation of new and revised policies and procedures.

- Establishing a monitoring process against the IG standards and local action plan.

The Information Governance Sub Group holds a working document which has details descriptions of all facets of Information Governance including a gap analysis and action plan. Progress against this document and aspirations for future activity are reported annually to the eHealth and Information Support Group through the sub group's annual report.

11. ROLES AND RESPONSIBILITIES OF KEY STAFF AND GROUPS

Chief Executive

- Overall statutory responsibility for patient safety, governance and performance management.
- Accountable to the Board and the Scottish Government Health Directorates

The Board has delegated responsibility for Information Governance to the Executive Lead for Information Governance. Currently this role is held by the Director of Finance. In order to discharge this responsibility, the Director of Finance vice-chairs and works through the eHealth and Information Support Group (eISG)

Director of Finance

- Leads the implementation of information governance at operational and strategic levels.
- Vice chairs the eISG.
- Reports to the Board and Chief Executive.
- Executive Lead for information governance.
- Is the Senior Information Risk Owner for the Board

Director of Human Resources and Support Services

- Chairs the eISG.

Executive Directors and Senior Managers

- Responsible for driving forward the development and embedding information governance (including data protection and IT security) across their areas of responsibility. Responsible for reviewing and recording risk to all corporate-level objectives.

eHealth and Information Support Group

- *eHealth and Information Support Group* is a strategic level steering group, which takes a lead role in the development of the Board information governance framework and IM&T strategies. The eISG also plays a role in monitoring systems commissioning, implementation, performance and including risk management.
- eISG reports to the Clinical, Care and Professional Governance Committee (CCPGC) and also to the Board through the Director of Human Resources and Support Services and other Directors with specific remit in respect of patient confidentiality, data protection and wider IG issues.
- The group membership includes stakeholders not only from across the organisation but also from Shetland Islands Council
- Establishes sub groups to take forward specific projects such as new systems implementation.

Information Governance Sub Group

- The Information Governance Sub Group is a sub-committee of the eHealth and Information Support Group, and it reports to that group.
- The sub-group advises the eISG regarding aspects of Information Governance
- The sub-group prepares a work plan and periodically reports progress of its activity to the eISG

Data Sharing Partnership

- The Data Sharing Partnership provides advice to all of its partner organisations: NHS Shetland, Shetland Islands Council, and Police Scotland. For NHS Shetland this advice feeds into the eHealth and Information Support Group.
- The Partnership oversees all agreements to share information between organisations, including different branches of the NHS

Clinical Care and Professional Governance Committee

The Clinical, Care and Professional Governance Committee (CCPGC) is a formal sub-committee of Shetland NHS Board. It is chaired by a Non Executive Member of the Health Board. It reviews the approaches to Information Governance and Records Management taken by the Health Board and the Council, monitoring that these operate effectively and that action is taken to address any areas of concern.

Risk Management Group

Where applicable, the Risk Management Group will review specific incidents or issues relating to IG risk.

Responsibilities of Key Staff

Executive Management Team (EMT) is responsible for ensuring that the policy and its supporting standards and guidelines are built into local processes and that there is on-going compliance. EMT is also accountable for the communication about, and compliance with, Board Policy. Line Managers must ensure that staff are adequately trained and apply the appropriate guidelines.

All staff, whether permanent, temporary or contracted are responsible for ensuring that they are aware of the requirements incumbent upon them and for ensuring that they comply with these on a day to day basis. Every member of staff is responsible for any records or data they create and what they do with information they use.

- The Caldicott Guardian takes ultimate responsibility for the treatment of patient information. The role of Caldicott Guardian is held by the Medical Director
- The Data Protection Officer is responsible for the Data Protection register for Shetland NHS Board and the Board responsibilities under the Data Protection Act. The role of Data Protection Officer is held by the Director of Finance
- IT Security Officer has overall responsibility for the infrastructure, security and backup of information systems. The role of IT Security Officer is held by Head of IM&T and eHealth

12. COMMUNICATION

Communication of this policy will follow the principles and process outlined in the Shetland NHS Board *Communication Strategy.*

The Information Management and Technology (IM&T) Department maintains both Internet and intranet sites providing a portal for all staff, patients and service users to access related information.

Minutes, reports and all appropriate documentation from the activities of the eISG and IG sub group will be published on the intranet and Internet including changes to this policy and associated policy documents, procedures and guidance.

Disseminating Information to staff about this policy.

The Board recognises the importance of ensuring that staff are fully appraised of activities in respect of information security and wider IG principles.

All staff therefore:

- Will be able to raise issues relating to information security at the eHealth and Information Support Group (eISG) through one of the members of the group.
- Will be able to view minutes of the meetings on the Internet.
- Receive information at formal updates such as induction and compulsory refresher days in respect of changes/revisions to information security policy and procedures.

Monitoring and review of this policy

- The policy will be reviewed biannually through eISG to ensure that the guidance and procedures remain up to date. The detailed action plan will be reviewed at every eISG and scrutiny will be provided by the Clinical Care and Professional Governance Committee
- The eISG will play a monitoring role in respect of reviewing and analysing trends in incident reporting and root cause analysis. Where applicable, the Risk Management Group will also review specific incidents or issues relating to IG risk.
- Key performance indicators and assessment against the national IG standards will be described in a separate action plan which will also include where applicable, targets in respect of data protection and information security issues. This action plan forms part of the IG policy document and progress against the indicators will be reviewed quarterly through eISG.

13. SUPPORTING DOCUMENTS

The IG Policy refers to and works in the context of other Board policies and procedures:

Information Security Policy
IT Security Policy
Patient Confidentiality Policy
Records Management Policy
Data Quality Policy
Data Sharing Policy
Social Media Policy

All the above policies require periodic revision and have timetables for completion set and this will be described in the work plan for 2019-20.

14. ACTION PLAN – HIGH LEVEL

- Ensure that Information Governance is overseen continuously through the Information Governance Sub Group to the eHealth and Information Support Group.
- Align Information Governance monitoring tools and strategies with guidance from National Services Scotland Information Governance team. Self assessment of performance of IG will be continuously and cyclically reviewed to address IG issues.
- Periodically refresh the Information Governance Policy and its companion policies and procedures.
- Report Information Governance policy and progress to the Board
- Ensure that all IG policy is aligned with the Public Records (Scotland) Act 2011.
- Ensure that all IG policy is aligned with the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679)

15. POLICY BREACHES

From time to time there will be occasions when there is a breach of policy. All such incidents shall be recorded in the Board's Datix reporting system. If appropriate, issues may be taken forward using the Board's disciplinary policy.

16. CONCLUSION

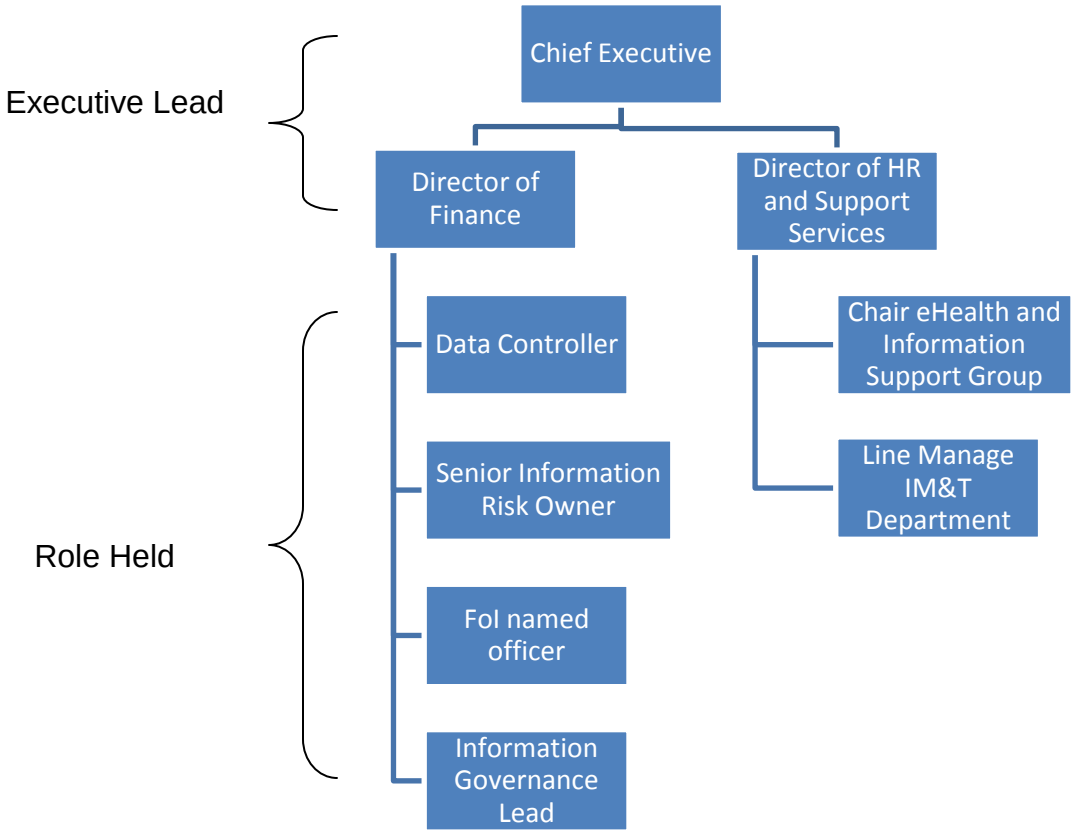
The implementation of the IG policy and action plan will ensure that information is more effectively managed within the Board. Each year the policy will be reviewed and an action plan developed against the IG standards to identify key areas for continuous improvement.

Appendix A

SHETLAND NHS BOARD
INFORMATION GOVERNANCE ORGANISATIONAL CHART 2019

Appendix B

Shetland NHS Board
Line Management of Key Roles in Information Governance



Appendix C

Membership of Information Governance Sub Group

Role	Named individual as at December 2018
Director of Finance	Colin Marsland
Interim Elective Services Manager	Janine Rochester
Data Protection Officer	David Morgan
Health of IM&T and eHealth	Craig Chapman
Information Manager	Stuart Hubbard
Health Records and Clinical Coding Manager	Pete Gaines
Corporate Services manager	Carolyn Hand

Membership of eISG

Role	Named individual as at December 2018
Director of HR and Support Services - Chair	Lorraine Hall
Director of Finance – Vice Chair	Colin Marsland
Medical Director	Brian Chittick
Designated Community Health and Social Care	Edna Mary Watson
Primary Care Manager	Lisa Watt
Health of IM&T and eHealth	Craig Chapman
eHealth Projects Lead	Andrew Carlyle
IT Team Lead	Michael Peterson
Information Manager	Stuart Hubbard
Executive Manager – AHP	Jo Robinson
Data Sharing manager	Jane Cluness
Clinical Governance Team Lead	Emma Garside
Designated acute services representative	Kate Kenmure
Health Records and Clinical Coding Manager	Pete Gaines
Corporate Services Manager	Carolyn Hand
Interim Elective Services Manager	Janine Rochester
Data Protection Officer	David Morgan

A continuously updated and more comprehensive version of staff in post is published online at https://www.shb.scot.nhs.uk/board/ig.asp

Appendix D: Equality and Diversity Rapid Impact Assessment

Information Governance Policy

<table>
<tr><td colspan="2">Rapid Impact Checklist: Summary Sheet</td></tr>
<tr><td>1. Positive Impacts (Note the groups affected)

Groups Affected:
1) NHS Shetland Staff
2) NHS Shetland patients

Impacts:
1) More appropriate treatment of patient information held by the Board
2) Better knowledge of information procedures amongst staff
3) Strengthens reputation of NHS Shetland.</td><td>2. Negative Impacts (Note the groups affected)

None identified</td></tr>
<tr><td colspan="2">3. Additional Information and Evidence Required

The Information Governance Policy does not have any particular impact on any group compared to any other group. However, some individuals may have difficulty in receiving or understanding the content of the procedure. These aspects are covered by the Board's Communication Policy.

The Information Governance Policy is a general policy which directs the content of other policies and protocols. All Shetland NHS systems will have their own specific protocols, and each of these will have their own equality and diversity assessment. Therefore specific equality and diversity concerns are addressed by the specific protocol.</td></tr>
<tr><td colspan="2">4. Recommendations

A full Equality and Diversity Impact Assessment is not required</td></tr>
<tr><td colspan="2">5. From the outcome of the RIC, have negative impacts been identified for race or other equality groups? Has a full EQIA process been recommended? If not, why not?

No negative impact has been identified
As no negative impact has been identified, a full EQIA process has not been recommended.</td></tr>
<tr><td colspan="2">Adopted by Information Support Group

Date: 17 January 2017</td></tr>
</table>