Birmingham and Solihull NHS
Mental Health NHS Trust

Information Governance Strategy

Document Reference:	IG01
Author:	Sandra Kelley
Version.Issue:	3.0
Status:	Final
Approved by:	Trust Board
Version date:	12th February 2007
Review date	February 2008

1 Introduction

1.1 This strategy describes the development and implementation of a robust Information Governance (IG) framework needed for the effective management and protection of organisational and personal information.

1.2 "Information Governance" describes the approach within which accountability, standards, policies and procedures are developed, implemented and maintained to ensure that all types of information used in the Trust are sourced, held and used appropriately, securely and legally.

1.3 Information is a vital asset for the trust, supporting both day to day clinical operations and the effective management of services and resources. Therefore it is essential that all Trust information is managed effectively within a robust governance framework.

1.4 The Trust requires accurate, timely and relevant information to enable it to deliver the highest quality health care and to operate effectively as an organisation. It is the responsibility of all staff to ensure that information is accurate and up to date and that it is used proactively in its business. Having accurate relevant information available at the time and place where it is needed, is critical in all areas of the Trust's business and plays a key part in corporate and clinical governance, strategic risk, service planning and performance management.

1.5 As a provider of health and social care, the Trust carries a responsibility for handling and protecting information of many types.

- Some information is confidential because it contains personal details of service users, their families or staff. The Trust must comply with legislation which regulates the holding and sharing of confidential personal information. It is important that relevant, timely and accurate information is available to those who are involved in the care of service users, but it is also important that personal information is not shared more widely than is necessary.

- Some information is non-confidential and is for the benefit of the general public. Examples include information about the Trust's services and information about mental health conditions and treatment options. The Trust and its employees share responsibility for ensuring that this type of information is accurate, up to date and easily accessible to the public.

- The majority of information about the Trust and its business should be open for public scrutiny although some, which is commercially sensitive, may need to be safeguarded.

2 Background

2.1 Information Governance is one of the main governance arrangements within the Trust i.e.

- Clinical Governance
- Risk Management
- Research Governance
- Financial Governance
- Information Governance

2.2 "Information Governance" covers all information held by the Trust (for example – clinical, staff, financial, estates, corporate, minutes) and all "information systems" used to hold that information. These systems may be purely paper-based or partially or totally electronic. The information concerned may be "owned" or required for use by the Trust and hence may be internal or external.

2.3 The governance requirements are intended to ensure that there is a robust framework concerning the obtaining, recording, holding, using, sharing and destruction of all data and records held or used by the Trust and ensuring that relevant information is available where and when it is needed.

2.4 Information Governance (IG) is considered under 7 themes -

- Information Governance Management
- Data Protection (including Caldicott)
- Confidentiality Code of Practice
- Care Records Management
- Freedom of Information and Corporate Records Management
- Information Quality Assurance
- Information Security

2.5 Information Governance contributes to the implementation of the Healthcare Commission's Standards for Better Health. It is specifically included in standards C9 and C13

> *C9 Health care organisations have a systematic and planned approach to the management of records to ensure that, from the moment a record is created until its ultimate disposal, the organisation maintains information so that it serves the purpose it was collected for and disposes of the information appropriately.*
>
> *C13 - Health care organisations have systems in place to ensure that*
> *….appropriate consent is obtained when required for all contacts with patients and for the use of any patient confidential information;*
> *….staff treat patient information confidentially, except where authorised by legislation to the contrary*

It contributes to other standards by ensuring that data required to support decisions, processes and procedures is accurate and available.

2.6 The Information Governance arrangements will underpin the Trust's strategic goals and ensure that the information needed to support and deliver their implementation is reliably available, accurate and understandable.

2.7 Implementation of robust Information Governance arrangements will deliver improvements in information handling by following the Department of Health standards (called the " HORUS model"), which requires information to be:

- **H**eld securely and confidentially
- **O**btained fairly and efficiently
- **R**ecorded accurately and reliably
- **U**sed effectively and ethically
- **S**hared appropriately and lawfully

2.8 Guiding principles

There are five interlinked principles which guide this IG Strategy:

- Openness
- Legal Compliance
- Information Security
- Quality Assurance
- Proactive use of information

2.9 In developing this IG Strategy, the Trust recognises and supports

- the need for an appropriate balance between openness and confidentiality in the management and use of information.

- the principles of corporate governance and public accountability and equally places importance on the confidentiality of, and the security arrangements to safeguard, both personal information about service users, families and carers and staff and commercially sensitive information.

- the need to share service user information with partner organisations (particularly health and social care) and other agencies in a controlled manner consistent with the interests of the service user and, in some circumstances, the public interest.

- the principle that accurate, timely and relevant information is essential to deliver high quality health and social care and that 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 Strategic objectives

3.1 Through implementing this strategy, the Trust will

- establish robust information governance processes conforming to the Department of Health standards

- ensure that all practices and procedures relating to handling and holding personal and Trust corporate information are legal and confirm to best and / or recommended practice

- ensure that clear advice is given to service users, families and carers about how their personal information is recorded, handled, stored and shared by the Trust and its partners. Service users will be provided with guidance, available in various formats, to explain their rights, how their personal information is handled, how they can seek further information and how they can raise concerns

- provide clear advice and guidance to staff and ensure that they understand and apply the principles of Information Governance to their working practice in relation to protecting the confidentiality and security of personal information and to ensuring the safe keeping and handling of Trust business information, ensuring compliance with appropriate legislation

- maintain a clear reporting structure and ensure through management action and training that all staff understand IG requirements

- undertake regular reviews and audits of how information is recorded, held and used. Management and Clinical Audits will be used to identify good practice and opportunities for improvement

- ensure procedures are reviewed to monitor their effectiveness so that improvements or deterioration in information handling standards can be recognised and addressed.

- ensure that when service developments or modifications are undertaken, a review is undertaken of all aspects of information governance arrangements to ensure that they are robust and effective

- work to instill an Information Governance culture in the Trust through increasing awareness and providing training on the key issues.

- ensure there are robust procedures for notifying and learning from IG breaches and incidents in line with the Trust's Risk Management Policy

- ensure service user participation in IG developments

- assess its own performance using the NHSIA Information Governance Toolkit and develop and implement action plans to ensure continued improvement

- in the future, assess its own performance using the social care Information Governance Toolkit (when it is operational) and develop and implement action plans to ensure continued improvement

3.2 To ensure **Openness,** the Trust will

- ensure that non-confidential information about the Trust and its services is readily and easily available through a variety of media, in line with the Trust's FOI Publication Scheme

- implement policies to ensure compliance with the Freedom of Information Act

- undertake or commission annual assessments and audits of its policies and arrangements for openness

- ensure that service users have readily and easily available access to information relating to their own care, their options for treatment and their rights as service users
- have clear procedures and arrangements for liaison with the press and broadcasting media
- have clear procedures and arrangements for handling queries from service users and the public

3.3 To ensure **Legal Compliance,** the Trust will

- regard all identifiable personal information relating to service users as confidential
- undertake or commission annual assessments and audits of its compliance with legal requirements
- regard all identifiable personal information relating to staff as confidential except where national policy on accountability and openness requires otherwise
- establish and maintain policies to ensure compliance with the Data Protection Act, Human Rights Act and the common law duty of confidentiality and all associated guidance
- establish and maintain policies for the controlled and appropriate sharing of service user information with other agencies, taking account of relevant legislation (e.g. Health and Social Care Act, Crime and Disorder Act, Protection of Children Act)

3.4 3.4 To ensure that appropriate and legal compliant **Information Systems Security** exists, the Trust will

- establish and maintain an Information Systems Security Policy along with respective procedures for effective policing and secure management of all its information assets, resources and IT systems
- undertake and/or commission annual assessments and audits of its information and IT security arrangements in-line with the said policy
- promote effective confidentiality and security practice to ensure all permanent/temporary, contracted staff and third party associates of the trust adhere to this via appropriate laid down policy procedures, training and information awareness schemes/documentation
- establish and maintain appropriate policing, incident reporting procedures and MIS monitoring and investigations of all instances, actual and/or potential, along with any reported breaches of confidentiality and security

3.5 To ensure **Information Quality Assurance,** the Trust will

- establish and maintain policies and procedures for information quality assurance and the effective management of records
- undertake or commission annual assessments and audits of its information quality and records management arrangements

- ensure that key service user data is accurately recorded and maintained, including regular cross-checking against source data
- ensure that managers are required to take ownership of, and seek to improve, the quality of information within their services and that information quality is assured at the point of collection
- ensure that data standards are set through clear and consistent definition of data items, in accordance with national standards.
- promote information quality and effective records management through policies, procedures/user manuals and training.

3.6 To ensure **proactive use of information**, the Trust will

- ensure information systems hold the information required to support clinical practice and operational management
- develop information systems and reporting processes which support effective performance management and monitoring
- develop information management awareness and training programmes to support managers in using information to manage and develop services
- support clinical, corporate, financial and research governance requirements
- promote an information culture and expectation of informed, evidence-based decision making
- ensure that, where appropriate and subject to confidentiality constraints, information is shared with other NHS, social care and partner organisations in order to support patient care

3.7 Implementation of this IG Strategy will ensure that the Trust and its staff handle and manage information in a consistent way. This is anticipated to lead to

- improvements in information handling activities
- reduction in numbers of IG incidents and complaints
- increased service user confidence in the NHS, the Trust and its staff

3.8 Information Governance provides a framework to bring together all of the requirements, standards and best practice that apply to the handling of personal and Trust information, ensuring

- compliance with the law and professional standards
- implementation of Department of Health advice and guidance
- year on year improvement

4 Information Governance roles and responsibilities

4.1. The Information Governance infrastructure consists of a steering group initially accountable to the Trust Board although this may change following the planned review of governance committees.There are 4 sub-groups which undertake detailed work in key areas.

4.2 The Trust Information Governance Steering Group (IGSG) is responsible to act on behalf of Trust Board for

- overseeing the implementation of this strategy
- the annual review of this strategy
- the development, approval and implementation of the associated policies and procedures in relation to the 4 sub-groups
- reviewing and signing off the IG work programme
- ensuring the accurate completion, review and sign off of the Information Governance Toolkit Assessment.

4.3 The IGSG will report progress quarterly to the Trust Integrated Governance Committee. It will also report quarterly to other committees as required.

4.4 There are 4 sub-groups responsible for

- Data Protection and Confidentiality Code of Practice
- Care Records Management
- Freedom of Information and Records Management
- Information Quality Assurance and Information Security

See figure 1.

4.5 The membership of the IGSG is

- Medical Director – Chair
- Director of Commercial Services and Asset Management
- Chairs of IG sub-groups
- Information Governance Lead Officer

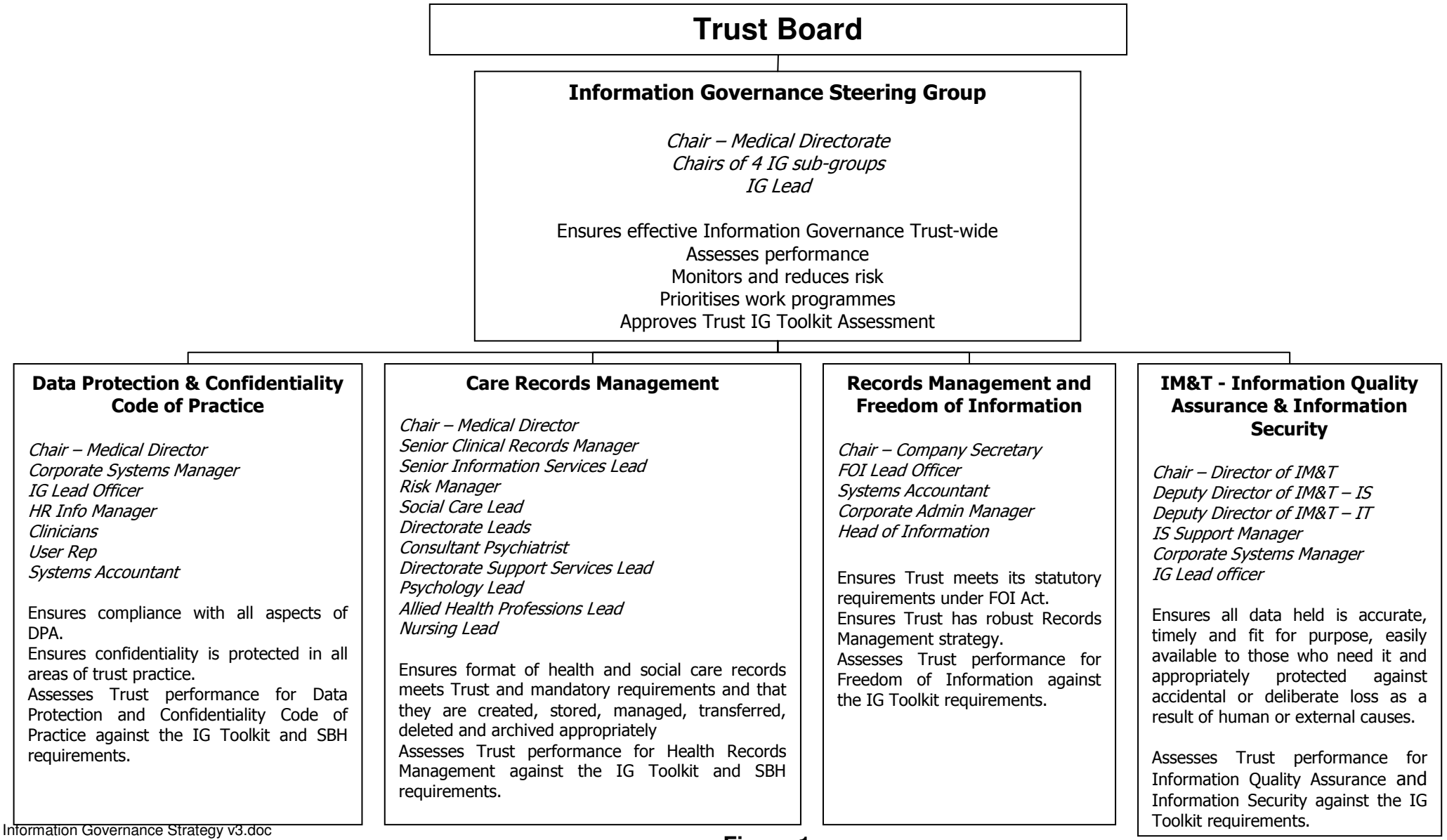
Trust Board
Information Governance Steering Group
Chair – Medical Directorate
Chairs of 4 IG sub-groups
IG Lead
Ensures effective Information Governance Trust-wide
Assesses performance
Monitors and reduces risk
Prioritises work programmes
Approves Trust IG Toolkit Assessment
Data Protection & Confidentiality Code of Practice
Chair – Medical Director
Corporate Systems Manager
IG Lead Officer
HR Info Manager
Clinicians
User Rep
Systems Accountant
Ensures compliance with all aspects of DPA.
Ensures confidentiality is protected in all areas of trust practice.
Assesses Trust performance for Data Protection and Confidentiality Code of Practice against the IG Toolkit and SBH requirements.
Care Records Management
Chair – Medical Director
Senior Clinical Records Manager
Senior Information Services Lead
Risk Manager
Social Care Lead
Directorate Leads
Consultant Psychiatrist
Directorate Support Services Lead
Psychology Lead
Allied Health Professions Lead
Nursing Lead
Ensures format of health and social care records meets Trust and mandatory requirements and that they are created, stored, managed, transferred, deleted and archived appropriately
Assesses Trust performance for Health Records Management against the IG Toolkit and SBH requirements.
Records Management and Freedom of Information
Chair – Company Secretary
FOI Lead Officer
Systems Accountant
Corporate Admin Manager
Head of Information
Ensures Trust meets its statutory requirements under FOI Act.
Ensures Trust has robust Records Management strategy.
Assesses Trust performance for Freedom of Information against the IG Toolkit requirements.
IM&T - Information Quality Assurance & Information Security
Chair – Director of IM&T
Deputy Director of IM&T – IS
Deputy Director of IM&T – IT
IS Support Manager
Corporate Systems Manager
IG Lead officer
Ensures all data held is accurate, timely and fit for purpose, easily available to those who need it and appropriately protected against accidental or deliberate loss as a result of human or external causes.
Assesses Trust performance for Information Quality Assurance and Information Security against the IG Toolkit requirements.

Figure 1

4.6 **Key roles and responsibilities**
The Medical Director is the named Executive Director on the Board with responsibility for Information Governance.

The Trust's Caldicott Guardian is the Medical Director.

The Trust's Data Protection Officer is the Deputy Director of IM&T – Information Services.

The Trust's Information Systems Security Officer is the Deputy Director of IM&T – IT Services

4.7 The Trust will involve service users and staff in the development of Information Governance arrangements. Initially this will involve communication and consultation on key topics with the Trust's PPI and encouraging service users to raise concerns particularly over confidentiality and access to information

5 Strategy implementation

5.1 The IGSG will monitor implementation of this strategy and its associated work programmes through regular meetings and through the IG sub groups.

5.2 All Trusts are mandated to complete a self-assessment of their IG performance using the NHS Information Authority IG Toolkit. This is an on-line self assessment tool based on 60 IG standards and is used as one of the sources of information by the Healthcare Commission for assessing compliance with Standards for Better Health, self improvement reviews etc. The Information Governance standards are based on generally accepted definitions of good practice in relation to information governance and inter-link with other recommendations and standards such as those in Standards for Better Health, CNST, the Data Protection Act etc.

5.3 Each IG sub-group will:

- undertake a baseline assessment of their current position in relation to their IG standards (using the self assessment toolkit)
- agree an annual work programme to ensure a year on year improvement in performance
- ensure the development of strategies, policies, procedures etc required for Information Governance
- identify resources required for implementation
- monitor progress made
- report on progress, incidents and issues to the IGSG
- assess their own performance against the IG toolkit on a quarterly basis
- complete the self assessment tool kit on an annual basis

5.4 The IGSG will review this strategy annually or in response to any significant changes to mandatory requirements, national NHS or social care guidance or as a result of significant information governance breaches or incidents.

6 Conclusion

The implementation of the Information Governance strategy, infrastructure and

action plans will ensure that all types of information is more effectively managed and proactively utilised at Birmingham & Solihull Mental Health NHS Trust.

7 Glossary / definitions

The following terms/acronyms are used within this document.

The Trust	Birmingham & Solihull Mental Health NHS Trust
ISG	Information Governance Steering Group
IG	Information Governance
NHSIA	National Health Service Information Authority
NCRS	NHS Care Records Service
C4H	Connecting for Health
NPfIT	National Program for Information Technology