WOKING & SAM BEARE
HOSPICES

INFORMATION GOVERNANCE FRAMEWORK (IGF)

Policy / procedure code:	IG 01
Version:	1.2
Ratified by:	Clinical Governance and Executive Committee
Name of policy owner:	SIRO
For Information and action to:	All WSBH employees and volunteers
Name of originator / author:	B Hamilton
Original issue date:	July 2015
Reviewed	October 2017
Next Review date:	September 20120

Version Control Sheet

Policy: Information Governance Framework

Version	Date	Author	Status	Comment
1	July 2015	B Hamilton	Ratified	Executive Team
1.1	July 2016	B Hamilton	Revised with addition of Data Flow Maps	C & CG Committees
1.2	Oct 2017	B Hamilton	Review / Proposed GDPR changes required	Corporate & Clinical Governance Committees

Signature Sheet
Policy: Information Governance Framework
Code: IG 01 **Version:** 1

Date	Name	Designation / Post	Department	Signature

Contents

Executive Summary

The Information Governance (IG) Strategy and associated policies outline Woking and Sam Beare Hospices (WSBH) commitment to comply with national IG standards, guidelines and regulations (Appendix 1) and implementing best practice. The Strategy is the overarching document for information governance within the organisation and links with other corporate policies dealing with the way that information is handled within the organisation

WSBH fully supports the principles of corporate governance and recognises its public accountability for confidentiality and security arrangements to safeguard, both service users personal information as well as commercially sensitive information. WSBH recognises the need to share service user information with other health organisations and agencies in a controlled manner consistent with the interests of the service user, of the business and, where appropriate, the public interest.

WSBH supports accurate, timely and relevant information as essential to deliver the highest quality health care. As such, it is the responsibility of all staff at all levels to ensure and promote the quality of information and to actively use information in decision-making processes.

1. Introduction

This strategy sets out the approach to management of information and states the legal basis for processing and storing personal and sensitive data . Information plays a key part in the WSBH Clinical and Corporate Governance. Quality of service provision and clinical and business decision making is reliant on accurate and available information. Public confidence in our ability to handle their data responsibly and efficiently is based on a good reputation for keeping data safe.

Information Governance (IG) relates to the responsible and effective handling of business and personal data in compliance with the Data Protection Act 1998 and the General Data Protection Regulation (GDPR) 2018 , Freedom of Information Act 2000, Department of Health Confidentiality: NHS Code of Practice and legal requirements under the, European Convention of Human Rights (Article 8 - Human Rights Act 1998) and common law. IG governance applies to all information (clinical and non-clinical) and all staff must understand their responsibility for effectively recording information and for keeping it secure and confidential.

The Information Governance Framework (IGF) is based on elements of law and policy from which IG standards are derived, and brings together all statutory, mandatory and best practice requirements for information management. The IGF defines the roles and individual and role responsibilities (trustees, board, floor level) which collectively ensure the defined standards are met.

The WSBH 2015/6 IGF and associated policies:

- Include standards for records management, information sharing, standards set in the NHS Information Governance Toolkit (IGT) and the General Data Protection Regulation (GDPR) 2018.
- Facilitate organisational planning to implement standards of practice as a foundation for every day, routine working practice and to measure and report compliance on an annually based on an annual work plan managed by the Corporate Governance Group.

- The action plan incorporates the following elements of IG
    - IG Management (management, accountability and responsibility)
    - Confidentiality & Data Protection Assurance (person identifiable information)
    - Information Security Assurance (manual/electronic information /records management)
    - Clinical Information Assurance (patient information/ records for direct clinical use)
    - Secondary Use Assurance (patient information/records, data quality, non-direct clinical use and training)
    - Corporate Information Assurance (Finance, Human Resources)

- Our aim is to achieve and maintain GDPR compliance and level 2 performance against all key NHS IG Toolkit requirements by March 2018.

2. Scope and Purpose

The purpose of this strategy is to ensure the people, processes, resources and culture are in place to support the core purpose of the organisation and ensure legal requirements are met.

The key components underpinning this strategy are:

- The Information Governance Policies which outline the IG standards.
- A dynamic action plan based on GDPR and NHS Information Governance toolkit (Voluntary Organisations) standards, regularly monitored and performance managed by the Corporate Governance Committee and operationalised by the IG Toolkit Working Group.
- Fundamental to the success of delivering the Information Governance strategy is developing an Information Governance culture within the organisation. Ongoing

awareness and training is required. Training plans are outlined in section 5.

3. Principles of Information Governance

DOH HORUS model principles: All information must be:

- Held securely and confidentially
- Obtained fairly and efficiently
- Recorded accurately and reliably
- Used effectively and ethically
- Shared appropriately and lawfully

3.1 Openness

- Non-confidential organisational information is available to the public through a variety of media, in line with WSBH code of openness.
- WSBH implement policies to ensure compliance with the Freedom of Information Act (i.e. obligations as a third party contractor to an NHS public body).
- Service users have ready access to information relating to their own health care and options for treatment under their rights as service users.
- WSBH will follow clear procedures and arrangements for handling queries from service users and liaison with the media.

3.2 Legal Compliance

WSBH will

- Regard all identifiable personal service user and personnel information as confidential except where national policy on accountability and openness requires otherwise.
- Undertake audits of its compliance with legal requirements.
- Establish and maintain policies to ensure compliance with the General Data Protection Regulation (GDPR), Data Protection Act, Human Rights Act and the common law of confidentiality.
- Establish and maintain policies for the controlled and appropriate sharing of service user information with other agencies, taking account of relevant legislation (Health and Social Care Act, Crime and Disorder Act, Protection of Children Act).

3.3 Information Security

WSBH will:

- Establish and maintain policies for the effective and secure management of its information assets and resources.
- Undertake audits of its information and IT security arrangements.
- Promote effective confidentiality and security practice to its staff through policies,

procedures and regular training.

- Establish and maintain incident reporting procedures and monitor and investigate all reported instances of actual or potential breaches of data protection, confidentiality and security.
- Ensure data base owners are aware of their responsibilities to maintain the files and data bases in their area of responsibility.
- Ensure data is held only as long as required by the original purpose for collecting the data by means of regular data cleansing from folders and data bases.

3.4 Information Quality Assurance

WSBH will:

- Establish and maintain policies and procedures for information quality assurance and the effective management of records.
- Undertake audits of its information quality and records management.
- Expect managers to take ownership of, and seek to improve, the quality of information within their services. Information quality should be assured at the point of collection.
- Set data standards through clear and consistent definition of data items, in accordance with national standards.

3.5 Communication principles

WSBH will:

- Ensure effective, systematic and consistent communication, at all levels.
- Demonstrate the organisation values and respects staff expertise and contributions, respects confidentiality, focuses on strengths and provides appropriate, balanced supervision, appraisal and evaluation.
- Provide clear and unambiguous communications in a language all parties understand.
- Ensure communications are two-way and participative, involving staff at all levels and the public in a meaningful dialogue illustrating WSBH is a learning organisation.
- Provide support to all staff in all their communications, through guidance, education and training.
- Provide a robust management and responsibility reporting structure to ensure IG risks are appropriately managed.
- Undertake regular reviews and audits of quality of information use.
- Provide clear advice and guidance in various formats via a Privacy Statement, website, information leaflets and posters to patients, families, carers and staff about how their personal information is used, recorded and shared and how any concerns may be raised.

3.6 WSBH Legal Basis for processing data

- Clinical Services - The lawful basis for processing and collecting data (Patient Identifiable) lies in Woking & Sam Beare registration as a registered Hospice (healthcare service provider). As such we have the right to use this information for administration of our clinical services.
- Charity - The lawful basis for processing and collecting data lies in Woking & Sam Beare registration as a registered Charity.

4. Responsibilities

Management Structure and Responsibilities	
	Responsibilities
Executive Board	- Ultimate responsibility for information governance and for ensuring that information risks are assessed and mitigated to an acceptable level and handled in a similar manner to other major risks such as financial, legal and reputational risks. - Completion of and sign off of the Annual IG Assessment (IG Toolkit) and Statement of Compliance (IGSOC) providing assurance of meeting key requirements and robust improvement plans in place to address any shortfalls. - Aware of serious incidents involving actual or potential loss of personal data or breach of confidentiality which must be published in annual reports and reported to the commissioners and to the Information Commissioner. - Define the WSBH policy in respect of IG (risk, legal and NHS requirements. - Ensure sufficient resources are available to support strategy implementation. - Responsibility is delegated via CEO (AO) to Director of Finance as SIRO.
Accountable Officer(AOIGOV)	- The WSBH AO (CEO) has overall accountability and responsibility for IG. - Provide assurance through the Statement of Internal Control that all risks IG risks are effectively managed and mitigated.
Data Protection Officer (DPO)	- Is an officer with professional experience and knowledge of data protection law proportionate to the type of processing carried out at WSBH and taking into consideration the level of protection the personal data requires.
Commissioning bodies	- Ensure all organisations, from which care is commissioned, achieve the IG Toolkit requirements.
Senior Information Risk Officer (S.I.R.O)	Responsible to the CEO (AO) for: - Strengthening controls around information governance and security. - Ownership of the organisation's IG risk, Information Risk Policy and risk assessment process and acts as advocate for IG risk on the Board. - Advise on the content of the Statement of Internal Control (information risk). - Ensure an effective information assurance governance infrastructure is in place including information asset ownership, Caldicott Guardian, reporting, defined roles and responsibilities and quality assurance of all records. - Provide a report to the Accountable Officer and Executive Board regarding the information risk/security content of the annual Statement of Internal Control (SIC) and annual report. - Chair the Information Governance Committee. - Authorise IG Toolkit Self-Assessment submissions. - Appoint and manage (in terms of information assets) of the IAO's. - Supported by Information Asset Owners (IAOs), IG Manager, IG Security

	Manager and Caldicott Guardian.
IG Manager / IT Manager (incl. security & governance)	- Manage the confidentiality and data protection components of the information governance toolkit, contributing to the annual assessment. - Ensure, along with the SIRO, that Information Asset Owners (IAOs) are nominated to manage local responsibilities under DPA and confidentiality within their work area. - Chair the Information Governance Steering Group. - Complete the annual Data Protection census and collates assurance evidence to support the submission of the IG Toolkit year-end report. - Maintain the WSBH's Data flow maps and Information Asset Register (IAR) - Provide advice and support on data protection and information security breaches. - Advise on, and maintains the WSBH's Information Sharing Agreements (ISA). - Support investigations into confidentiality breaches or potential breaches with relevant IAOs/IAAs; ensures reports and action plans are presented to the IT & Information Governance Committee for monitoring of completion. - Provides monthly reports to the Information Governance Committee on caldicott and data protection matters for wider communication. - Advise where updates are required to WSBH's Data Protection Registration status and maintains the register. - Maintain a register of all IT applications / databases containing Personal Confidential Data (PCD) registered under the WSBH global notification (The Data Protection Act 1998). Before personal data can be held on computer, it is necessary to notify the Information Commissioner's Office. - Ensure effective information assurance governance infrastructure is in place including information asset ownership, reporting, defined roles and responsibilities. - Provide expert technical advice on matters relating to IT Security and ensure compliance and conformance
Information Asset Owner (I.A.O)	- Accountable to the SIRO for providing assurance on the security and use of the information assets within their respective area are identified, recorded and controls are in place to mitigate any risks. - Support the SIRO in the overall information risk management function. - Identify, understand and address risk to the information assets they "own". - Responsible for operational management of WSBH records according to policy. - Complete and maintains WSBH Information Asset Register. - Responsible for appointing Information Asset Administrators (IAAs). Working with IAAs to ensure they share a clear understanding of responsibilities and accountabilities relating to asset ownership. Especially vital where information assets are shared by multiple parts of the WSBH. - Ensure actual or potential breaches of confidentiality are reported on Sentinel and investigated to ensure lessons are learned and changes in practice occur.

Information Asset Administrators (IAAs)	- Support I.A.O in the delivery of their information risk management responsibilities. - Ensure policies and procedures are followed. - Recognise actual or potential security incidents and mitigate those risks. - Consult their IAO on incident management. - Ensure information asset registers are accurate. - Undertake follow-up reviews of failed log-in reports within their systems and reporting failures to their line management and on Sentinel. - Ensure security risks are controlled, risk assessments are in place detailing control measures and that these are regularly reviewed.
Caldicott Guardian	- IG 'conscience' of the organisation actively supporting work to enable information sharing where this is appropriate and advising on lawful and ethical solutions. - Focal point for patient confidentiality issues. - Champion confidentiality and information sharing requirements and issues at Board level within the WSBH's overall governance framework. - Act in a strategic, advisory and facilitative capacity in the use and sharing of patient information. - Ensure WSBH and partner agencies satisfy best practice standards. - Review and authorise information sharing agreements and requests for PCD disclosure. - Maintain registration with the Health and Social Care Information Centre (HSCIC). - Approve, monitors and reviews protocols governing access to person identifiable information by WSBH staff and other organisations. - Advise on the options for lawful and ethical processing of information.
IG Committees	- Steering the WSBH IT and IG agenda - Develop, maintain and approve policies, standard procedures, training and guidance. - Coordinate and raise awareness of IG. - Report on an exception basis to the WSBH Board on IG risk issues. - Support the SIRO in completion his/her duties. - Direct and monitor compliance with GDPR compliance and NHS IG Toolkit standards. - Oversee the implementation of the IG strategy /annual IG improvement plan. - Report to the Corporate Governance Committee. - Report the result of self-assessment audits to the WSBH Board for approval. - Challenge the performance report and ensure appropriate actions are taken. - Owner of the IG Risk register in relation to IG risks. Identifies new risks and reviews progress on reducing current risks on the WSBH's risk register. - Oversee the implementation of the WSBH's information governance

	work programme (including DP & Confidentiality and Caldicott work plans).
IG Steering Group	- Oversee day to day Information Governance issues including incidents, audits and risks. - Progresses the annual IG Action Plan. - Implements the IG improvement plan
Directors	- Fully aware of IG Policy contents and responsibility for implementation. - Responsible for IG in their areas of responsibility. - Ensure effectiveness and integration of IG arrangements. - Active involvement in IG Committee and IG agenda - Fostering an IG culture.
Managers	- Ensuring policy, standards and guidelines are built into local processes to secure compliance. - Ensure all job descriptions contain the relevant responsibility for information security, confidentiality and records management. - Ensure staff undertake IG mandatory training and assess ongoing training needs. - Individually responsible for the security and management of WSBH records within their respective area/department wherever information is processed and stored.
All staff (permanent, temporary, contracted, students, contractors, volunteers)	- Understand and apply best practice and the principles of IG to manage all information to support WSBH. - Comply with information security policy and procedures including maintenance of data confidentiality, data integrity and ensure that no breach of information security or confidentiality, result from their actions. Failure may result in disciplinary action. - Maintain accurate records. - Operational security of the information systems they use. - Undertake relevant information governance training.
Third Party Contractors/third parties	- Appropriate contracts and confidentiality/ information security agreements shall be in place with third party contractors/ third parties where potential or actual access to information assets is identified.

5. Education, Training, Development (IG ETD) and Guidance

All staff must understand the value of information and their responsibility for it, including data quality, information security, records management, confidentiality, legal duty, information law and rights of access in terms of a right of privacy and choice.

- Staff may not access WSBH ICT systems without first receiving IG awareness training.
- Different levels of training available include:
  - Introductory level for all staff at induction
  - Foundation level for staff who handle personal information routinely.
  - Practitioner level for those in IG specialist roles.
  - Mandatory basic IG Training is a mandatory requirement for all staff.
  - Guidance material is available via the staff IG handbook.
- The following principles will apply:
  - All staff receive training in the areas of IG specified by IG toolkit requirements.
  - Staff induction programmes highlight IG aspects including confidentiality, data protection, Caldicott and Freedom of Information (FOI) awareness.
  - Specific detailed IG training is available for key staff, where appropriate.
  - IG will be considered in all training programs.

6. The annual IG Toolkit work program

- Is dependent upon the latest version of the HSCIC Information Governance Toolkit.
- Performance is self-assessed using the IG Toolkit and scoring assured by internal audit.
- The Corporate Governance Committee will drive progress on the IG toolkit.

Appendix 1 Legislation and Guidance

WSBH must ensure that all policies and procedures are fully compliant with legislation and NHS guidance on the management of information, including (but not limited to) the following:

- General Data Protection Regulation (GDPR) 2018
- Access to Health Records Act 1990 and Guidance for Access to Health Records Requests February 2010 (Gateway Reference 13214).
- Data Protection Act 1998.
- Human Rights Act 1998.
- Freedom of Information Act 2000.
- Department of Health Records management: NHS code of practice Parts 1 and 2. 2013.
- NHS Codes of Practice.
- Computer Misuse Act 1990.
- Crime and Disorder Act 1998.
- Regulations of Investigatory Powers Act 2000.
- Electronic Communications Act 2000.
- Department of Health Information Governance Toolkit. V 9 2014.
- ISO27001 (formally ISO/IEC 17799:2000,BS 7799 Information Security).

Appendix 2 Definitions & Information

Definitions:

- **Information governance** is the framework of law and best practice that regulates the manner in which information, including information relating to and identifying individuals, is managed (i.e. obtained, handled, used and disclosed).
- **Information Asset** a body of information defined and managed as a single unit so it can be understood, shared, protected and exploited effectively. Information assets have recognisable and manageable value, risk, content and lifecycle.

IG Toolkit

- An online system which allows NHS organisations and partners to assess themselves against DOH Information Governance policies and standards.
- All providers are required to achieve a minimum of level 2 performance against key requirements published through the NHS Information Governance Toolkit
- The annual information governance assessment is measured via a self-assessment process of compliance against the standards set out in the NHS Information Governance Toolkit and assur Internal Audit. The standards are ordered into the following initiatives:
  - Information Governance Management
  - Information Security Assurance
  - Confidentiality and Data Protection Assurance
  - Clinical Information Assurance
  - Secondary Use Assurance
  - Corporate Information Assurance
- From 2009/10 onwards, organisations were required to submit three IG performance reports to the DOH, which can be tracked by Commissioners and other monitoring bodies.

The NHS Connecting for Health IG Statement of Compliance

- All organisations wishing to access and use NHS CFH systems and services, including the N3 network, must meet the terms and conditions in the IG Statement of Compliance (IGSoC
- The IGSoC is the agreement between NHS CFH and Approved Service Recipients that sets the information governance policy and terms of conditions for use of NHS CFH services.
- The IGSoC contains a number of obligations which aim to preserve the integrity of these services, which requires:
- No patient identifiable data or other sensitive data is stored or processed offshore, where the location is deemed noncompliant with the NHS CFH Offshore Policy
- The right of audit by NHS CFH or nominated third parties
- Change Control Notification procedures and approval processes
- Organisations to achieve or be working towards ISO27001
- Organisations report security events and incidents
- The IGSoC process is supported by annual completion of the IG Toolkit with a minimum level 2 performance against all key requirements

The NHS Care Record Guarantee

- Sets out the rules that govern patient information held within the NHS Care Record Service, but as they are derived from statute and common law the guarantee also applies to patient data held on legacy systems. It is owned by the National Information Governance Board for Health and Social Care. The Guarantee covers:

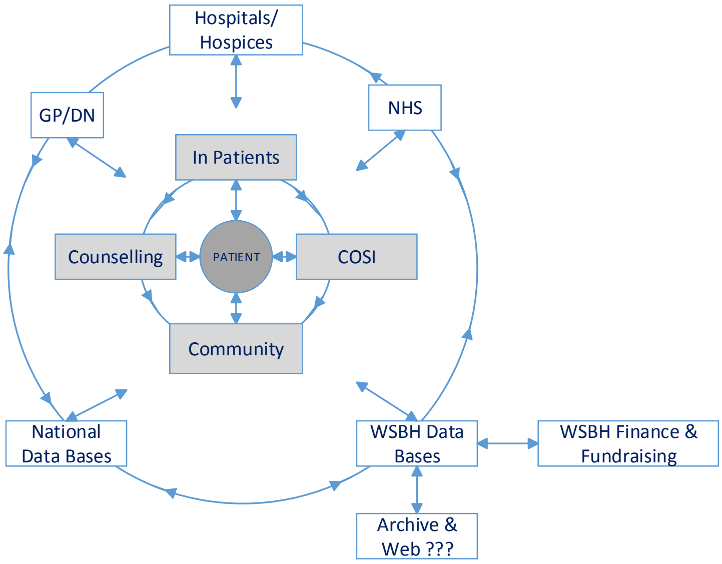
- Peoples' right of access to their own records
  - How access will be monitored and policed
  - Options people have to limit access
  - Access in an emergency and the procedure about control and use when someone cannot make decisions for themselves
- Emphasises and strengthens the NHS's clear commitment to confidentiality and security of patient's information, which WSBH shall adhere to by compliance with the Confidentiality and Data Protection Assurance standards set out in the Information Governance Toolkit.

The Privacy Agenda

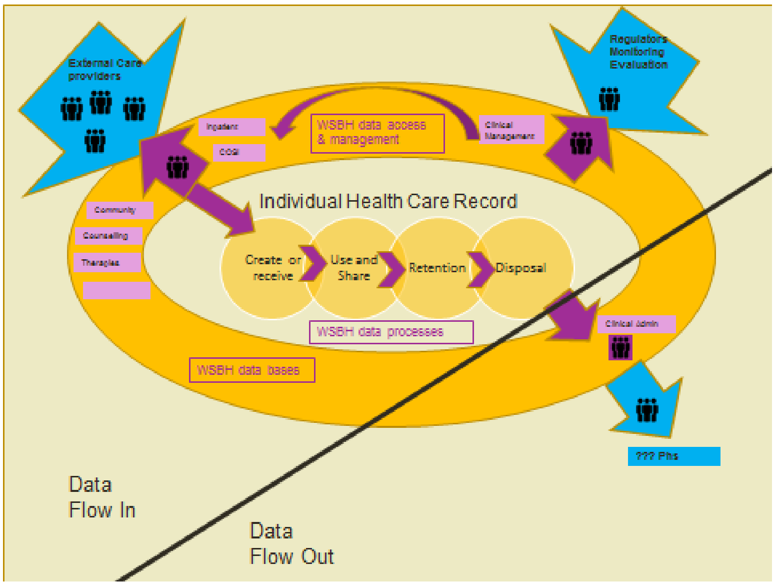
- The Data Protection Act 1998 protects personal data through the application of eight principles.
- Privacy is about a patient's right to decide whether or not to divulge sensitive information known only to them and who should know it.
- Patients expect staff to keep their private information confidential and can specify who can and who cannot have access to it and what it may or may not be used for.
- WSBH staff must ask the patient to consent before their personal data can be used for non-healthcare purposes such as research or management purposes. This should be updated when the patient's condition changes e.g. community patient admitted to IPU.
- There are two specific areas of strategic IG strategy that address the privacy agenda – the Confidentiality and Data Protection Assurance agenda standards that relate to the NHS Care Record Guarantee (National Information Governance Board 2009) and Privacy Impact Assessments and the NHS Pseudonymisation Project (PIP).
- Sharing should be only on a need-to-know basis.
- Patients have a right of access to their health records, a right to know who has accessed their record and a right to consent/dissent to information being shared.
- The development of electronic care records will include (at some point) technical components that control and restrict access to patient data.

Appendix 3 WSBH High Level Data Flow Map & Clinical Operations Flow Map

WSBH HIGH LEVEL DATA FLOW MAP



Clinical Operational Data Flow


External Care providers
Regulators Monitoring Evaluation
Inpatient
COSI
WSBH data access & management
Clinical Management
Community
Counselling
Therapies
Individual Health Care Record
Create or receive
Use and Share
Retention
Disposal
WSBH data processes
WSBH data bases
Clinical Admin
??? Phs
Data Flow In
Data Flow Out