Cheshire and Wirral Partnership
NHS Foundation Trust

Document level: Trustwide (TW)
Code: IM10
Issue number: 7

Information Governance Policy

Lead executive	Medical Director & Caldicott Guardian
Authors details	Trust Records & Information Governance Manager/DPO

Type of document	Policy
Target audience	All CWP staff
Document purpose	To provide a statement of the Trust's approach to information governance and to inform staff of their responsibilities.

Approving meeting	Information Governance & Data Protection Sub-Committee	09-Oct-19
Implementation date	09-Oct-19	

CWP documents to be read in conjunction with	
HR6	Mandatory Employee Learning (MEL) policy
IM1	ICT Acceptable Usage Policy (AUP)
IM3	Data quality policy
IM4	Standards for secondary use of information policy
IM5	Information asset register policy
IM6	Information sharing policy
IM7	Code of confidentiality policy
CP3	Health records policy
CP63	Access to health records policy
GR1	Incident reporting and management policy
GR3	Risk management policy
GR12	Media policy
GR17	Freedom of information Policy
GR41	Corporate records policy
HR3.3	Disciplinary policy and procedure
HR13	Registration authority policy
FR1	Integrated governance strategy

Document change history	
What is different?	Section 2 Updated links to policies Section 2 & 3 updated reference to Records & Information Systems Group to Information Governance & Data Protection Sub-Committee Section 3 updated information governance framework to reflect corporate governance structure Section 3.1.4 included Caldicott Champion function to roles
Appendices / electronic forms	Not applicable
What is the impact of change?	Not applicable

Training requirements	Select - Training requirements for this policy are in accordance with the CWP Training Needs Analysis (TNA) with Education CWP.

Document consultation	
Clinical Services	Clinical representatives of the Information Governance & Data Protection Sub-Committee
Corporate services	Corporate representatives of the Information Governance & Data Protection Sub-Committee
External agencies	None

Financial resource implications	None

External references
1.

Equality Impact Assessment (EIA) - Initial assessment	Yes/No	Comments
Does this document affect one group less or more favourably than another on the basis of:		
- Race	No	
- Ethnic origins (including gypsies and travellers)	No	
- Nationality	No	
- Gender	No	
- Culture	No	
- Religion or belief	No	
- Sexual orientation including lesbian, gay and bisexual people	No	
- Age	No	
- Disability - learning disabilities, physical disability, sensory impairment and mental health problems	No	
Is there any evidence that some groups are affected differently?	No	
If you have identified potential discrimination, are there any exceptions valid, legal and/or justifiable?		
Not applicable		
Is the impact of the document likely to be negative? - If so can the impact be avoided? - What alternatives are there to achieving the document without the impact? - Can we reduce the impact by taking different action?	No N/A N/A N/A	
Where an adverse or negative impact on equality group(s) has been identified during the initial screening process a full EIA assessment should be conducted. If you have identified a potential discriminatory impact of this procedural document, please refer it to the human resource department together with any suggestions as to the action required to avoid / reduce this impact. For advice in respect of answering the above questions, please contact the human resource department.		
Was a full impact assessment required?	No	
What is the level of impact?	N/A	

Contents

1. Introduction to information governance 4
1.1 Data Security & Protection Toolkit....4
2. Information governance principles 4
2.1.1 Openness 4
2.1.2 Legal compliance....4
2.1.3 Information security....5
2.1.4 Information quality assurance 5
2.2 Information governance policy scope....5
2.2.1 Information types 5
2.2.2 Information processing....5
2.2.3 Information assets....5
2.3 Monitoring and review....6
2.3.1 CWP information governance structure....6
3. Information governance management framework 6
3.1 Information governance: key role descriptions 7
3.1.1 Chief Executive....7
3.1.2 Senior Information Risk Owner (SIRO) 7
3.1.3 Caldicott Guardian 8
3.1.4 Information Governance Lead....10
3.1.5 Information Asset Owners (IAO) 11
3.1.6 Managers....11
3.1.7 Staff (including staff of partner and sub-contractor organisations)....12
3.1.8 Contractors and service suppliers....12

Appendix 1 - Abbreviations....13

1. Introduction to information governance

Cheshire and Wirral Partnership NHS Foundation Trust (CWP) acknowledges that information is a vital asset both to the delivery of high quality clinical care and to the efficient management of services and resources. Information governance describes the systems, processes and behaviours which support the Trust in managing its information assets.

Robust information governance requires clear and effective management and accountability structures; governance processes; documented policies and procedures; trained staff and adequate resources. This policy documents the CWP's approach to meeting these requirements and reflects the national NHS Digital's Data Security & Protection Toolkit (DSPT) a mandatory annual assessment of information governance performance.

1.1 Data Security & Protection Toolkit

Compliance against national standards for information governance is monitored through the annual DSPT assessment encompasses the National Data Guardian review's 10 data security standards. The requirements of the DSPT also support key requirements under the General Data Protection Regulation (GDPR).

The DSPT is updated annually and all larger NHS organisations are normally required to make three submissions – a baseline in July, interim in October and a final assessment in March. Performance against the DSPT is published by NHS Digital. The DSPT submission is examined by the Trust's regulators: The Care Quality Commission (CQC) review the toolkit assessment in their assessments while the foundation trust regulator, NHSI, consider the toolkit when assessing the foundation trust's governance risk rating.

2 Information governance principles

CWP recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. CWP fully supports the principles of corporate governance and 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. CWP also recognises the need to share patient information with other health organisations and agencies in a controlled manner consistent with the interests of the patient and in some circumstances the public interest (see Information Sharing Policy).

CWP believes that accurate, timely and relevant information is essential to deliver the highest quality healthcare. 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.

2.1.1 Openness

- Non-confidential information about CWP and its services is available to the public through a variety of media;
    - CWP will adhere to the Freedom of Information Policy to ensure compliance with the Freedom of Information Act;
- CWP will undertake annual assessments / audits of its policies and arrangements for openness;
- Patients will have ready access to information relating to their own healthcare, their options for treatment and their rights as patients (see Access to Health Records Policy);
- CWP will adhere to procedures and arrangements for liaison with the press and broadcasting media (see Media Relations Policy);
- CWP will adhere to procedures and arrangements for handling queries from patients and the public (see Access to Health Records Policy and Freedom of Information Policy).

2.1.2 Legal compliance

- CWP regards all identifiable personal information relating to patients as confidential;

- CWP will undertake or commission annual assessments / audits of its compliance with legal requirements;
- CWP regards all identifiable personal information relating to staff as confidential except where national policy on accountability and openness requires otherwise;
- CWP will adhere to policies to ensure compliance with Data Protection Legislation, Human Rights Act and the common law duty of confidentiality (see Access to Health Records Policy);
- CWP will adhere to policies for the controlled and appropriate sharing of patient information with other agencies, taking account of relevant legislation (e.g. Health and Social Care Act, Crime and Disorder Act, Protection of Children Act), see Information Sharing Policy.

2.1.3 Information security

- CWP will establish and maintain policies for the effective and secure management of its information assets and resources;
- CWP will undertake annual assessments / audits of its ICT security arrangements;
- CWP will promote effective confidentiality and security practice to its staff through policies, procedures and training;
- CWP will adhere to incident reporting procedures and will monitor and investigate all reported instances of actual or potential breaches of confidentiality and security (Risk Management Policy, Confidentiality Policy and Health Records Policy)

2.1.4 Information quality assurance

- CWP will establish and maintain policies and procedures for information quality assurance and the effective management of records;
- CWP will undertake or commission annual assessments / audits of its information quality and records management arrangements;
- Managers are expected to take ownership of and seek to improve the quality of information within their services;
- Wherever possible, information quality should be assured at the point of collection;
- Data standards will be set through clear and consistent definition of data items, in accordance with national standards;
- CWP will promote information quality and effective records management through policies, procedures / user manuals and training see data quality policy.

2.2 Information governance policy scope

Information governance applies to all data processes and equipment used to manage information for which CWP is accountable.

2.2.1 Information types

This policy covers all information including, but not limited to:

Person-Identifiable Information	Organisational Information
Service user / carer / client / patient	Commercially sensitive
Staff / contractor / partner / stakeholder	Planning, research and development
Member / governor / patient and public representative	Publicly available

2.2.2 Information processing

This policy applies to the lifecycle management (creation, storing, processing, transmission, archiving and destruction) of all CWP information, in any format or medium. Also see Health Records Policy and Corporate Records Policy. .

2.2.3 Information assets

This policy applies to all information assets – data, reports, systems, software, hardware, staff, contractors and suppliers involved in the management or use of CWP information. To support staff

and contractors working within the requirements of information governance, see Information Asset Register Policy.

2.3 Monitoring and review

Information governance is embedded within the governance structure of CWP and linked to information governance across local health communities. The Information Governance & Data Protection Sub-Committee (IG&DPSC) will review as standing agenda items:

- Breaches of confidentiality;
- Inappropriate access to electronic clinical systems;
- System security;
- Subject access requests;
- Freedom of information requests.

Breaches of confidentiality and CWP policy will result in disciplinary action in accordance with the CWP Disciplinary Policy and Procedure

The formal structure supporting information governance is set out below:

2.3.1 CWP information governance structure

Board of Directors (BOD)
Chair: Chairman

▼

Operational Committee (Ops Committee)
Chair: Chief Executive

▼

Information Governance & Data Protection Sub-Committee (IG&DPSC)
Chair: Medical Director, Effectiveness & Medical Workforce

▼

Task and finish groups convened as requested

Compliance with this policy and delivery of any associated action plans will be monitored by the Ops Committee which may delegate authority for certain monitoring aspects to IG&DPSC.

The policy will be reviewed and approved through IG&DPSC. Reviews will be either triggered by changes to legislation or material changes to regulation and guidance or mandated governance changes, or when the review date is due.

3. Information governance management framework

Heading	Requirement	CWP Response (appointed leads / document approval dates)
Senior roles	- Information Governance Lead - Senior Information Risk Owner (SIRO) - Caldicott Guardian	- Records & IG Manager/DPO - Finance Director - Medical Director (Effectiveness & Medical Workforce)
Key policies	- Information Governance Policy - Confidentiality Policy - Freedom of Information Policy - Information Sharing Policy - Information Asset Register Policy - Health Records Policy - Access to Health Records Policy - Corporate Records Policy - Registration Authority Policy	IG&DPSC

Heading	Requirement	CWP Response (appointed leads / document approval dates)
	- Data Quality Policy - ICT Policy - Clinical Coding Policy - Mobile Devices Policy - Secondary Use of Information Policy	
Key governance bodies	IG&DPSC Care Group Governance Meetings	Ops Committee & Quality Committee
Resources	Budget	There is no single identifiable budget for information governance, other than staff costs. Funding for initiatives PR projects is either identified from existing departmental budgets or from the approval of business cases.
	Staff	SIRO (Director of Finance) Caldicott Guardian (Medical Director) Information Governance Lead (Records & IG Manager/DPO) Caldicott Guardian Support Function (Records Manager & IG Manager / Data Protection Officer / Privacy Officer) - Head of Corporate Affairs (FOI) - Head of Information (Data Quality)
Governance framework	- Duties and Responsibilities - Contract Clauses - Information Asset Owner (IAO)	- Information Governance Policy - Standard Staff Contracts - SIRO
Training and guidance	- DSPT - IG training tool - IG policies and procedures - Code of Conduct	- Confidentiality Policy
Incident management	- Incident Reporting and Management Policy - Incident reporting system - Datix (Trustwide) - Incident reporting monitoring	- Trimester report to Quality Committee - Escalation risk and incident report to board of directors (BOD) - Annual information governance report to BOD

3.1 Information governance: key role descriptions

3.1.1 Chief Executive

The accounting officer for CWP is the chief executive who has overall responsibility for ensuring that appropriate and effective systems of information governance are in place throughout the Trust.

3.1.2 Senior Information Risk Owner (SIRO)

Information Risk Owner (SIRO) should be an Executive Director or other senior member of the Board. The SIRO may also be the organisations Chief Information Officer (CIO) if the latter is on the board but should not be the Caldicott Guardian as the SIRO should be part of the organisation's management hierarchy rather than being an advisory role.

The CWP SIRO is an executive director (currently the director of finance) who highlights the impact on Trust strategy of information risks. The SIRO appraises the board of information risks and advises on information risk in the statement of internal control. Information Asset Owners (IAOs) are accountable to the SIRO.

The SIRO will be expected to understand how the strategic business goals of the organisation may be impacted by information risks and it may therefore be logical for this role to be given to a Board member already leading on risk management or information governance.

The SIRO will act as an advocate for information risk on the Board and in internal discussions and will provide written advice to the Accounting Officer on the content of the annual Statement of Internal Control (SIC) in regard to information risk.

The SIRO will provide an essential role in ensuring that identified information security risks are followed up and incidents managed and should have ownership of the Risk Management Policy and associated risk management strategy and processes. The SIRO will provide leadership and guidance to the organisation's Information Asset Owners (IAO).

Information risk issues will be escalated to the SIRO from the Information Governance & Data Protection Sub-Committee.

The SIRO is required to successfully complete strategic information risk management training at least annually.

Key responsibilities are to:

- Oversee the development of a Risk Management Policy and a strategy for implementing the policy within the existing information governance framework;
- Take ownership of the risk assessment process for information risk, including review of an annual information risk assessment to support and inform the Statement of Internal Control;
- Review and agree action in respect of identified information risks;
- Ensure that the organisation's approach to information risk is effective in terms of resource, commitment and execution and that this is communicated to all staff;
- Provide a focal point for the resolution and /or discussion of information risk issues;
- Ensure the Board is adequately briefed on information risk issues.

3.1.3 Caldicott Guardian

The Caldicott guardian is a senior clinician (currently the medical director, effectiveness and medical workforce) who oversees the use and sharing of patient information, championing confidentiality and information sharing within and outside the Trust. The guardian plays a key role in ensuring that the Trust satisfies the highest practical standards for handling patient-identifiable information. The Guardian should be: an existing member of the senior management team or a senior health or social care professional or the person with responsibility for promoting clinical governance or equivalent functions.

Acting as the "conscience" of an organisation, the guardian actively supports work to enable information sharing where it is appropriate to share and advises on options for lawful and ethical processing of information.

The Caldicott guardian also has a strategic role, which involves representing and championing confidentiality and information sharing requirements and issues at senior management level and where appropriate, at a range of levels within the organisation's overall governance framework. The role is particularly important in relation to the implementation of the National Programme for IT and the development of electronic social care records and common assessment frameworks.

In all but the smallest organisations, the Caldicott guardian should work as part of a broader Caldicott function with support staff, Caldicott or information governance leads etc. contributing to the work as required.

Accountable to: Chief Executive

Job summary: The appointment of a Caldicott Guardian was one of the recommendations of the Caldicott report published in December 1997. The role of the guardian is to safeguard and govern uses made of patient information within the Trust, as well as data flows to other NHS and non-NHS organisations. Caldicott guardianship is a key component of broader information governance.

The guardian is responsible for the establishment of procedures governing access to, and the use of, person-identifiable patient information and, where appropriate, the transfer of that information to other bodies.

In addition to the principles developed in the Caldicott report, the guardian must also take account of the codes of conduct provided by professional bodies, and guidance on the protection and use of patient information and on IM&T security disseminated by the Department of Health, including the NHS Confidentiality Code of Practice

Working relationships
The Caldicott Guardian will be expected to liaise and work with service managers and the Trust Board in the course of promoting the Caldicott principles, which will include attendance at various meetings as appropriate.

The Caldicott Guardian is the chair of the Information Governance & Data Protection Sub-Committee. The Caldicott Guardian is expected to work closely with records management, HR, ICT, and other colleagues from work areas represented on that group.

Through an established network of NHS and Social Services representatives, the Caldicott Guardian also contributes to the peer review and interpretation of local or national confidentiality issues and the development of standards throughout the local health and social care community and partner organisations.

The Caldicott guardian is supported by the information governance lead and Caldicott support function.

Time commitment
The amount of time spent on Caldicott work will vary from week to week depending on scheduling of meetings and ad hoc demands etc.; however it is estimated that on average the time commitment will equate to one clinical session per week (1 SPA).

Key tasks
Production of procedures, guidelines and protocols

- To oversee development and implementation of procedures that ensure that all routine uses of person-identifiable patient information are identified, agreed as being justified and documented;
- To oversee development and implementation of criteria and a process for dealing with ad hoc requests for person-identifiable patient information for non-clinical purposes;
- To ensure standard procedures and protocols are in place to govern access to person-identifiable patient information;
- To work with the research, research ethics and clinical audit committees and personnel to ensure protocols for releasing information for research and audit are in line with applicable information governance standards;
- To understand and apply the principles of confidentiality and data protection as set out in the DH publication `Confidentiality: NHS Code of Practice', and, where current practice falls short of that required, to agree challenging and achievable improvement plans.

Information for staff

- To ensure standard information governance procedures and protocols are in an understandable format and available to staff;

- To ensure raised awareness, through training and education, of the standards of good information governance practice and Caldicott principles and that they are understood and adhered to.

Information sharing to support care

- To work with other care providers and linked agencies to facilitate better sharing of relevant information about patients, in a manner that facilitates joined-up care across institutional boundaries while ensuring that patients' legal rights and the Caldicott principles are maintained;
- To that end, ensure establishment of information sharing protocols, in line with guidance provided by the Department of Health, to govern the use and sharing of patient-identifiable information between organisations both within and outside the NHS;
- In collaboration with the Records & Information Governance Manager/DPO and ICT department, to draw to the attention of all staff through raising general awareness (trustwide email bulletins, team brief and any other suitable means at disposal) correct practices in relation to person identifiable patient information, following specific incidents where procedures, guidelines and protocols have been breached by staff.

Strategic

- To ensure that the Trust, in its development of strategy and process to implement the various elements of the NHS Digital guidelines, maintains its compliance with Caldicott Principles and other relevant legislation;
- Specifically this will include, but not be limited to:
    - Advising on staff registration and authentication processes;
    - Assignment of appropriate role profiles to staff;
    - Advising on workgroup construction for access control purposes;
    - Ensuring that confidentiality alerts and audit trail monitoring are effectively managed.
- To keep abreast of developments within NHS Digital, and in particular the opportunities for safeguarding patient information through promoting use of anonymised or coded data obtained via the Secondary Uses Service (SUS).

Reporting

- In collaboration with the information governance lead and Caldicott Support Function, to draw to the attention of the relevant manager any occasion where the appropriate procedures, guidelines and protocols may have not been followed;
- To raise concerns about any inappropriate uses made of patient information with the board of directors and / or chief executive where necessary;
- On an annual basis, to participate in the Data Security & Protection Toolkit assessment (adherence to the standards are included in the trust's performance ratings);
- Also on an annual basis, to formally report to the board of directors the trust's performance against the whole IG agenda, making recommendations for further improvement where appropriate.

3.1.4 Information Governance Lead

The information governance lead is accountable for ensuring effective management, accountability, compliance and assurance for all aspects of information governance. They have operational responsibility for the delivery of a sound and effective information governance system.

Key tasks include:

- Developing and maintaining the currency of comprehensive and appropriate documentation that demonstrates commitment to and ownership of information governance responsibilities;
- Ensuring there is top level awareness and support for information governance resourcing and implementation of improvements;

- Providing direction in formulating, establishing and promoting information governance policies;
- Establishing working groups to co-ordinate the activities of staff given information governance responsibilities and progress initiatives;
- Ensuring annual assessments and audits of information governance policies and arrangements are carried out, documented and reported;
- Ensuring that that annual assessment and improvement plans are prepared for approval by the senior level of management in a timely manner;
- Ensuring that the approach to information handling is communicated to all staff and made available to the public;
- Ensuring that appropriate training is made available to staff and completed as necessary to support their duties in line with the informatics planning component of the NHS operating framework;
- Liaising with other committees, working groups and programme boards in order to promote and integrate information governance standards;
- Monitoring information handling activities, including access to confidential information, to ensure compliance with law and guidance;
- Providing a focal point for the resolution and / or discussion of information governance issues.

Caldicott Guardian Support Function

- Providing general support to Caldicott Guardian in relation to confidentiality issues;
- Providing general support to Trust staff in relation to confidentiality issues;
- Review appropriate IG policies;
- Provide breaches of confidentiality reports to the IG&DPSC;
- Maintain data protection registration for the Trust;
- Act as privacy officer for summary care record.

Caldicott Champions

- Providing general support to Caldicott Guardian within care group in relation to confidentiality issues and promoting good Caldicott practice within care group.

3.1.5 Information Asset Owners (IAO)

For information risk, IAOs are directly accountable to the SIRO and provide assurance that information risk is being managed effectively for their assigned information assets. They may be assisted in their roles by staff acting as Information Asset Administrators (IAAs) who have day to day responsibility for management of information risks affecting one or more assets.

Each IAA should be aware of what information is held, and the nature of the justification for information flows to and from the assets for which they are responsible.

The role of the IAO is to understand what information is held, what is added and removed, how information is moved, who has access and why. As a result they should be fully able to understand and address risk to the information and ensure that information is fully used within the law for the public good.

The IAO will be responsible for providing or informing regular written reports to the SIRO a minimum of annually on the assurance and usage of their assets.

It is important that ownership of information assets is linked to a post rather than a named individual to ensure that responsibilities for the asset are passed on should the post holder leave the organisation or change jobs within it.

3.1.6 Managers

- Managers are responsible for ensuring that their staff are aware of their information governance responsibilities. That they have appropriate access to training and support and act in accordance with Trust policies and procedures in all aspects of information governance. Managers must report information incidents in accordance with the Trust's Incident Reporting and Management Policy

and recognise and manage information risk according to the CWP's Risk Management Policy. Managers are responsible for ensuring that contracts for staff or services meet CWP policies and procedures for information governance. Managers are responsible for ensuring that a Data Protection Impact Assessment is completed before new processes or information assets that might impact on information security, confidentiality and data protection, and information quality are introduced.

3.1.7 Staff (including staff of partner and sub-contractor organisations)

All CWP employees and employees of partner and sub-contractor organisations must ensure that they undertake mandatory information governance training, access support and abide by all relevant policies and procedures. Information risks must be managed and information incidents reported through the CWP's Incident Reporting and Management Policy and Risk Management Policy.

3.1.8 Contractors and service suppliers

All contractors and service suppliers must act in accordance with legislation and adhere to CWP policies and procedures at all times. Information must not be removed from the organisation in any form without the written consent of CWP and must be disposed of in accordance with CWP policy.

Appendix 1 - Abbreviations

CQC	Care Quality Commission
IAA	Information Asset Administrator
IAO	Information Asset Owner
DSPT	Data Security & Protection Toolkit
Ops Committee	Operational Committee
IG&DPSC	Information Governance & Data Protection Sub-Committee
SIRO	Senior Information Risk Owner
SPA	Supporting Professional Activities