EAST LANCASHIRE HOSPICE

INFORMATION GOVERNANCE POLICY

Aims

- Compliance with legislation relating to Information Governance
- Compliance with the NHS Information Governance Toolkit at Level 2
- Compliance with Care Quality Commission Standards

Supporting Standard Operating Procedures (SOP)

- Data Processing
- Privacy Statements
- Consent
- Storing Personal Data Securely
- Ensuring Accuracy And Quality Of Personal Data
- Disclosure, Sharing And Transfer Of Personal Data Including Rectification
- Retention, Archiving And Destruction Of Information
- Management Of Data Subject Access Requests
- Information Governance Information, Training And Support
- Contractual Arrangements Regarding Information Governance
- Audit and Managing Information Governance Risk
- Considering Information Governance Implications For New Developments, Information Systems And Assets
- Payment Card Industry Data Security Standard (PCI DSS) Compliance

Appendix

1. Information Governance Management Framework
2. Data Subject Rights

Approved by:	Corporate Governance
Date:	March 2012
Author:	Development and Support Services Manager
Version:	Final October 2018

Scope:	All staff, volunteers, and students on placement, those working under practicing privileges and contractors

Policy File:	Corporate	**Date of Ratification:**	March 2012
Policy No:	P020	**Date Launched:**	October 2018
		Review Date:	October 2019

1. Policy Statement

1.1 This policy and the supporting Standard Operating Procedures (SOP) detail how East Lancashire Hospice complies with legislation and best practice guidance in regard to information governance.

1.2 This policy provides direction for all employees, either employed directly or via a contractor and volunteers, whose duties include the handling of 'personal data' and 'sensitive personal data', which is processed by the hospice.

1.3 The hospice recognises the need for an appropriate balance between openness and confidentiality in the management and use of information. The hospice fully supports the principles of information governance and recognises its public accountability, equal emphasis is placed on the importance of confidentiality and the security arrangements to safeguard, both personal information and commercially sensitive information. The hospice 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.

1.4 The hospice 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.

1.5 There are four key interlinked principles to the Information Governance policy: Openness, Legal Compliance, Information Security and Quality Assurance.

2. Definitions

2.1 **IT:** Information Technology such as computers, laptops, internet and social media.

2.2 **Information Governance:** Information governance is a framework to ensure information is handled legally, securely, efficiently and effectively in order to deliver the best possible services.

2.3 **Confidentiality:** Maintaining the privacy of information ensuring disclosure is with consent or authorised under legal requirements.

2.4 **Senior Information Risk Owner (SIRO):** Senior Manager who takes ownership of the organisation's Information Risk Policy and Information Risk Management Strategy. At East Lancashire Hospice this is the Development and Support Services Manager.

2.5 **Data Protection Officer:** Senior Manager responsible for monitoring internal compliance, providing advice and acts as a point of contact for data subjects. At East Lancashire Hospice this is the Development and Support Services Manager.

2.6 **Caldicott Guardian:** Senior Manager responsible for protecting the confidentiality of patient and service-user information and enabling appropriate information-sharing. At East Lancashire Hospice this is the Clinical Services Manager.

2.7 **Information Asset Owner (IAO):** Individual responsible for specified information, at East Lancashire Hospice, Service Managers are IAO's for their services.

2.8 **Data Controller:** An organisation or legal entity who decides the purpose(s) for which personal data or sensitive personal data is processed is known as a 'data controller'. It is the duty of the data controller to comply with the requirements of the Data Protection Act and associated legislation. The controller is responsible for, and must be able to demonstrate, compliance with the principles.

2.9 **Data Processor:** A data processor acts on behalf of the Data Controller - this relates to all staff and volunteers who process data on behalf of the hospice and data processors sourced from external organisations.

2.10 **Data Subject:** The data subject or 'subject' describes the individual about whom personal data or sensitive personal data has or will be collected. This includes patients, next of kin/carers, service users, customers, staff, volunteers, donors, supporters and contractors.

2.11 **Personal Identifiable Information (PID)/Personal Data:** This means any information relating to a living individual who may be identifiable from that information. Personal data can be factual information about an individual, such as name, address and telephone number, or it can be an expression of opinion about an individual in addition on line identifiers such as an IP address can be considered personal data.

2.12 **Sensitive Personal Information (SPI)/Sensitive Personal Data (SPD):** Information which specifically relates to an individual's racial or ethnic origin, political affiliation(s), financial details, religious beliefs, physical/mental health, sexual life, and criminal allegations/convictions.

2.13 **Processing:** The use of the term 'processing' in this policy refers to obtaining, recording, using, altering, storing, transmitting, disclosing or destroying personal data or sensitive personal data. stored electronically which includes computer records, digital photographs/images held on a computer or manually in the form of structured paper files e.g. lists, printed spreadsheets, letters, faxes, printed photographs etc.

2.14 **Disclosure:** This term refers to any information divulged verbally, electronically or in writing, including intended and unintended disclosures.

2.15 **Breach:** Incident where there is failure to comply with legislation or best practice for example an unintended disclosure or cyber security attack.

2.16 **Consent:** Permission to obtain and process data, this should be; freely given, specific, informed and an unambiguous indication of the individual's wishes. There must be some form of clear affirmative action – or in other words, a positive opt-in – consent cannot be inferred from silence, pre-ticked boxes or inactivity. Consent must also be separate from other terms and conditions, and there needs to be simple ways for people to withdraw consent.

2.17 **Privacy Notice:** A way to describe the information made available or provided to individuals when information is collected about them and includes how information will be used and processed. Privacy notices should comply with the ICO code of practice privacy notices, transparency and control.

2.18 **Health Record:** 'Consists of information relating to the physical or mental health or condition of an individual, and has been made by or on behalf of a health professional in connection with the care of that individual'. They can be held in a variety of media for a variety of functions.

2.19 **Information Commissioner Office (ICO):** Upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals.ICO is an executive non-departmental public body, sponsored by the government.

3. Key Principles

3.1 Personal data is obtained fairly and efficiently, collected for specified, explicit and legitimate purposes and be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

3.2 Data subjects understand how personal information is used and shared and are fully informed of their rights via privacy statements.

3.3 Personal data is held securely and confidentially, processed in a manner that ensures protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

3.4 Personal data is processed lawfully and the conditions for lawful processing are identified before obtaining information.

3.5 Personal data is processed lawfully, fairly and in a transparent manner in relation to individuals and not further processed in a manner that is incompatible with those purposes for which it was obtained.

3.6 Personal data is used effectively and ethically, recorded accurately and reliably and, where necessary, kept up to date.

3.7 Every reasonable step is taken to ensure that personal data that is inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

3.8 Personal data is shared appropriately and lawfully, it is kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Arrangements are in place to support and promote information sharing for coordinated and integrated care. Information is transferred in an effective, secure and safe manner.

3.9 Destruction/deletion of personal data is carried out effectively in line with retention periods.

3.10 There is an adequate Information Governance Management Framework to support the current and evolving information governance agenda.

3.11 Employees and volunteers understand their responsibilities for information governance and have the information, training, support and resources to do this effectively.

3.12 There are formal contractual arrangements that include compliance with information governance requirements, in place with all contractors and support organisations that have access to the organisation's information or conduct any form of information processing on its behalf.
3.13 The hospice conducts regular audit of its compliance with this policy to provide assurance of compliance with legislation and best practice requirements via the governance structure.
3.14 Risks and breaches are managed effectively ensuring reporting, review and reduction of risk that contributes to organisational learning.
3.15 All new processes, services, information systems, and other relevant information assets are developed and implemented in a secure and structured manner, and comply with information governance security accreditation, information quality and confidentiality and data protection requirements.
3.16 There is consistent and comprehensive use of the NHS Number in line with National Patient Safety Agency requirements.
3.17 An organisational Information Asset Register is compiled and reviewed annually by the DPO and IAO's
3.18 The hospice conforms to NHS Information Governance Toolkit at level 2

4. Responsibilities

4.1 Board of Trustees

4.1.1 Ensure sufficient resources are available to implement this policy and associated SOP.
4.1.2 Through representation at the Corporate Governance Committee seek assurance that this policy and associated Standard Operating Procedures are being effectively implemented across the organisation.
4.1.3 Through Quarterly Management Reports be aware of developments, concerns or actions regarding information governance.

4.2 Corporate Governance Committee Responsibilities

4.2.1 Take account of the DPO's advice and the information provided on compliance with legal obligations and best practice guidance
4.2.2 Allocate responsibility for action regarding reduction of Information Governance risks to relevant Members of the Senior Management Team.
4.2.3 Approve this policy, SOP and associated documentation.

4.3 Information Governance Lead: DPO/SIRO/Information Security Manager Responsibilities (Development and Support Services Manager)

4.3.1 Monitor Compliance with GDPR and other data protection laws, policies, training and audit.
4.3.2 Carry out Data Protection Impact Assessments with the responsible IAO.
4.3.3 Act as point of contact for the ICO, cooperating with ICO as required.
4.3.4 Have due regard to the risks associated with processing operations, taking into account the nature, scope, context and purposes of processing.
4.3.5 Be an easily accessible point of contact for our employees, individuals and ICO.
4.3.6 Provide information, education and advice to support the organisation in achieving compliance within legislation, and best practice in regard to information governance.
4.3.7 Produce and update this policy and associated procedures and documentation.
4.3.8 Ensure the Senior Management Team and BOT are aware of resources and action required to ensure effective information governance via the governance structure.
4.3.9 Conduct regular audit of information governance practice.
4.3.10 Develop, maintain and upload evidence to achieve the requirements of the NHS Standard Contract, of achieving level 2 compliance with the NHS Information Governance Toolkit.
4.3.11 Report breaches in accordance with SIRI's Guidance.
4.3.12 Consider information governance implications for new developments, information systems and assets that are commissioned.

4.3.13 Provide reports to the Corporate Governance Committee to give assurance that this policy and associated SOP are being effectively implemented in practice and highlighting any risks or concerns requiring action.

4.4 Caldicott Guardian Responsibilities (Clinical Services Manager)

4.4.1 A strategic role, acting as the 'conscience' for the organisation, in regard to personal information relating to patient information. This involves representing and championing confidentiality and information sharing requirements and issues actively supporting and advising on options for lawful and ethical processing of healthcare information. Ensuring that the highest practical standards for handling patient information are implemented.

4.4.2 Take into account the findings and recommendations from Dame Fiona Caldicott's second review of Information Governance in 2013 (the Caldicott2 Review) in decision making.

4.4.3 Work with the Information Governance Lead internally and Information Asset Owners in other organisations, to manage information governance issues reacting to patients.

4.5 Senior Management Team Responsibilities

4.5.1 Senior Managers are the Information Asset Owners for the personal data obtained, stored, processed, used, transferred, disclosed, shared, archived and destroyed in their services, they are responsible for ensuring this policy and associated SOP is applied in practice and that they seek and take account of the DPO's advice and any information provided on compliance with legal obligations and best practice guidance to ensure effective information governance.

4.5.2 Update the organisational Information Asset Register ensuring inclusion of or all information obtained, stored, processed, used transferred, disclosed, shared, archived and destroyed in their service.

4.5.3 Support the DPO in conducting audits to monitor the effective implementation of this policy and SOP in practice within their service areas and progress any actions identified to achieve compliance with legislation and best practice.

4.5.4 Keep up to date with national and local requirements specific to their services in regard to information governance, informing the Information Governance Lead and Corporate Governance Committee of any requirements and how it is proposed to implement these in practice.

4.5.5 Ensure staff and volunteers in their service access information, education advice and resources to support them in implementing this policy and associated SOP in practice.

4.5.6 Ensure all new staff and volunteers in their services are aware of this policy and SOP and include how these relate to their role and implementation in practice in the individual induction plan.

4.5.7 Report concerns, breaches and risk to the SIRO/Information Governance lead in line with the SOP, ensuring risks are reviewed for any breaches relating to their services and take appropriate action to reduce future risk and improve practice.

4.5.8 Ensure contractual arrangements regarding information governance are in place for any SLA/contracts they are responsible for.

4.5.9 Consider information governance implications for new developments, information systems and assets that are commissioned for use in their service.

4.6 Heads of Department

4.6.1 Ensure this policy and associated SOP are implemented in practice to ensure effective information governance of all personal data obtained, stored, processed, used, transferred, disclosed, shared, archived and destroyed in their department.

4.6.2 Provide accurate updates to their Service Manager to ensure the services Information Asset Register accurately reflects information held within their own department.

4.6.3 Support the DPO and Service Managers in conducting audits to monitor implementation of this policy and SOP in practice within their department.

4.6.4 Ensure staff and volunteers in their department have access to information, education, advice and resources to support them in implementing this policy and associated SOP in practice.

4.6.5 Report concerns, breaches and risk in line with the SOP, review risks and breaches in their department and take appropriate action to reduce future risk and improve practice.

4.6.6 Consider information governance implications for new developments, information systems and assets that are commissioned for use in their department.

4.7 Employee, Volunteer Responsibilities

4.7.1 Familiarise themselves with this policy and SOP to understand how these relate to their role on commencement and thereafter when reviewed.

4.7.2 Access information, education, and advice to equip them in effectively implementing this policy and SOP.

4.7.3 Act in accordance with this policy and SOP as relevant to their role.

4.7.4 Report concerns, breaches and risk in line with the SOP, review risks and breaches and take appropriate action to reduce future risk and improve practice.

5. References

5.1 This policy and associated SOP and documents refer to regulations and industry codes of practice which impact on the processing of personal data. These include but are not limited to:

- The General Data Protection Regulations (2018)
- The Data Protection Act (1998)
- The Common Law Duty of Confidence
- The Confidentiality NHS code of Practice
- The NHS Care Record Guarantee for England
- The Social Care Record Guarantee for England
- International Information Security Standard ISO/IEC27002:2005
- The Information Security NHS code of Practice
- Information Governance Alliance (2016) The Records Management code of Practice for Health and Social Care
- The Freedom of Information ACT (2000)
- NMC Standards on Record Keeping
- Privacy & Electronic Communication regulations (PECR)
- Access to Health Records Act 1990, c.23
- Health & Social Care Act 2008,
- ICO Guidance and Codes of Practice
- NHS Information Governance Toolkit
- Goddard Inquiry recommendations regarding retention Jan 2016
- NHS Information Governance Toolkit

EAST LANCASHIRE HOSPICE
Standard Operating Procedure

Data Processing

1. Overview

1.1 Personal data must be obtained fairly and efficiently, collected for specified, explicit and legitimate purposes and be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. Above and beyond this requirement, where the personal information concerned falls within special category, additional condition for processing under Article 9 of the GDPR (2018) must also be identified.

1.2 Fair processing requires organisations to be transparent – clear and open with individuals about how their information will be used and shared. Assessing whether information is being processed fairly depends partly on how it is obtained. In particular, if anyone is deceived or misled when the information is obtained, then this is unlikely to be fair.

1.3 To assess whether or not personal data is processed fairly, consideration must be given to how it affects the interests of the people concerned – as a group and individually. If the information has been obtained and used fairly in relation to most of the people it relates to but unfairly in relation to one individual, there will be a breach of the first data protection principle.

1.4 Why and how personal data is collected and used will be relevant in assessing fairness which requires the organisation to:

- Be open and honest about your identity
- Tell people how you intend to use any personal data you collect about them (unless this is obvious)
- Usually handle their personal data only in ways they would reasonably expect; and
- Above all, not use their information in ways that unjustifiably have a negative effect on them.

2. Process

2.1 Identifying Conditions for Lawful Processing

Process
Personal data should only be obtained if one or more of the 6 conditions for lawful processing, detailed below, are met • With the explicit consent of the data subject, unless reliance on consent is prohibited by EU or Member State law • For the performance of a contract with the data subject or to take steps to enter into a contract • Necessary for compliance with a legal obligation • Necessary to protect someone’s life • Necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller • Necessary for the purposes of legitimate interests pursued by the controller or a third party, except where such interests are overridden by the interests, rights or freedoms of the data subject
The IAO will identify the condition for lawful processing for all types of personal information relevant to their service and document this on the Information Asset Register
Rationale
The lawful conditions for obtaining personal data is considered and recorded.

2.2 Informing People about Their Rights Regarding Information

Process
People's rights regarding information are detailed in **Appendix 3** and are presented on the hospice website, in the hospice statement of purpose to inform individuals about their rights in regard to the use of their personal information
This is supported by explanations provided by the staff who process data as they are able to answer queries or refer individuals to someone who can such as the IAO, Caldicott Guardian or Lead for Information Governance
Where it is identified that a data subject has special/different needs an individualised approach will be used by the IAO so that communications are tailored to meet their needs
Rationale
• Data subjects are aware of their rights.

2.3 Objections to Processing

Process
Individuals have the right to object to processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling); direct marketing (including profiling); and processing for purposes of scientific/historical research and statistics. The individual's right to object will be highlighted at the point of first communication and be explicit in the privacy notice
Objections to processing should be directed to the DPO who will consider the request with the IAO and respond on a case by case basis
Individuals must have an objection on "grounds relating to his or her particular situation" which should be respected unless: it can be demonstrated that there are compelling legitimate grounds for the processing, which override the interests, rights and freedoms of the individual; or the processing is for the establishment, exercise or defence of legal claims
We will stop processing personal data for direct marketing purposes as soon as we receive an objection. There are no exemptions or grounds to refuse. An objection to processing for direct marketing will be dealt with at any time and free of charge
Rationale
Centralised point for dealing with requests Compliance with legislation.

2.4 Restricted Processing

Process
Requests to restrict processing should be directed to the DPO who will consider the request with the IAO and respond on a case by case basis
Restriction of the processing of personal data is required in the following circumstances: • Where an individual contests the accuracy of the personal data, the processing will be restricted until the accuracy of the personal data has been verified • Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and consideration is being given as to whether the organisation's legitimate grounds override those of the individual • When processing is unlawful and the individual opposes erasure and requests restriction instead • If the personal data is no longer required but the individual requires the data to establish, exercise or defend a legal claim If the personal data in question has been disclosed to third parties, they must be informed inform about the restriction on the processing of the personal data, unless it is impossible or involves disproportionate effort to do so Individuals will be informed when a decision is made to lift a restriction on processing
Rationale
Centralised point for dealing with requests Compliance with legislation.

2.5 Rectification

Process
Individuals are entitled to have personal data rectified if it is inaccurate or incomplete
All requests for rectification must be sent to the Information Governance Lead who will work with the relevant information asset own to respond
If the personal data in question has been disclosed to third parties, they must be informed of the rectification where possible. The individuals must also be informed about the third parties to whom the data has been disclosed where appropriate
A response will be sent within one month of the request. This can be extended by two months where the request for rectification is complex
If a decision is made that no action is to be taken in response to a request for rectification, an explanation will be provided to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy
Rationale
Centralised point for dealing with rectification Compliance with legislation.

Privacy Statements

1. Overview

1.1 Individual's have a right to be informed about the collection and use of their personal data. This is provided via a privacy statement and includes:

- Name and details of the organisation
- Name and contact details of DPO
- Purpose for processing
- Lawful condition for processing
- Legitimate interests - where applicable
- Categories of personal data
- Who it will be shared with
- Retention details
- Rights of the individual.
- Identifying conditions for lawful processing

2. Process

2.1 Provision of Privacy Notices

Process
Privacy notices are displayed on the hospice website, in key information literature and on forms where PID is collected
Privacy notice information is also provided orally by staff involved in collection of PID
This layered approach allows the hospice to provide both general information and specific information in more detailed to data subjects
Privacy information is provided in clear straightforward language
Privacy information is available at the point PID is collected
Privacy information is monitored and audited annually
Rationale
Compliance with ICO guidance.

Consent

1. Overview

1.1 Consent must be a freely given, specific, informed and unambiguous indication of the individual's wishes. There must be some form of clear affirmative action – or in other words, a positive opt-in – consent cannot be inferred from silence, pre-ticked boxes or inactivity.

1.2 Consent must also be separate from other terms and conditions, and you will need to provide simple ways for people to withdraw consent. Public authorities and employers will need to take particular care to ensure that consent is freely given.

1.3 Consent has to be verifiable, and individuals generally have more rights where you rely on consent to process their data.

1.4 Remember that you can rely on other lawful bases apart from consent – for example, where processing is necessary for the purposes of your organisation's or a third party's legitimate interests.

2. Process

2.1 Consent

Process
IF NO OTHER CONDITION FOR LAWFUL PROCESSING CONSENT MUST BE OBTAINED IAO need to ensure there are clear, concise, specific and explicit opt-in methods of consent with robust records and simple easy-to-access ways for people to withdraw consent. Consent is seen as an organic, ongoing and actively managed choice, and not simply a one-off compliance box to tick and file away
The IAO should ensure that there are clear concise and explicit written statements of consent to process personal information informing people of : • What personal information is required • Who will have access to it • How it will be processed • Whom it may be transferred to and for what purpose • How it will be kept safe and secure • How long it will be kept for • How it will be destroyed • How they can withdraw consent
When asked to provide personal information people should sign that they understand the statement of consent
The statement of consent will be retained by the IAO until the end of the retention period for that information
All data subjects whose information is used for direct marketing will opt into having their information used in this way
Rationale
Compliance with legislation.

EAST LANCASHIRE HOSPICE
Standard Operating Procedure

Storing Personal Data Securely

1. Overview

1.1 The organisation must protect the security of all data it holds ensuring only those authorised to access the information are able to do so.

2. Procedure

2.1 General Security

Process
The hospice general security is audited annually
Computers and paper records are based in rooms with secure windows and doors that are locked when rooms are not in use
IAO are responsible for ensuring effective security of the information they own
Staff are responsible for the security of the information they process
Rationale
• Security is maintained.

2.2 Security of Paper Records

Process
All paper based records containing PID or SID are stored in locked cabinets, drawers or rooms with access restricted to specified individuals with authority to access that information
Paper records are never left unattended or on view
The hospice operates a clear desk policy and all work stations should be cleared of confidential information when the desk is not occupied
Rationale
• Security of paper records is maintained.

2.3 Security of Medical Records

Process
The majority of medical records are electronic and on the EMiS system, which is an NHS system with in-built security features. Access is via an individualised password authorised by the IAO for the System - The Clinical Services Manager. The system has also has time out feature and one touch closure
Historic paper medical records are stored in locked rooms without windows - these can be accessed by request from Clinical Administration and a tracking system is in place
Medical notes for IPU patients are stored in a lockable trolley in the IPU office which is also lockable when no one is in the room and non ELH medical records are stored in a cabinet within a secure room when not in use
Rationale
• Security of medical records is maintained.

2.4 Security of Computer Systems and Electronic Records

Process
A Registration Authority (MLCSU) manages the registration and access control processes required to ensure that individuals who need to access computer systems have their identity rigorously checked. This is vital as the hospice is linked to the NHS Spine. Users are assigned appropriate access according to the business need - this is provided to the hospice under a service level agreement
Network controls exist to protect the local network from threats to its components. This includes the systems and applications using the network, as well as the information passing through it, and the level of access

permitted. This is provided to the hospice by MLCSU under a service level agreement
Anti-virus software is installed on all computers and updates are carried out regularly. This is provided to the hospice by MLCSU under a service level agreement
Monitoring and enforcement processes are in place to ensure NHS national application Smartcard users comply with the terms and conditions of use. This is provided to the hospice by MLCSU under a service level agreement
All computers are accessed by named user with their own password, specific to the individual. Passwords must not be shared
Computer users log out when leaving the computer unattended. Log in details and passwords are not written down
Screens are positioned to minimise the risk of others seeing confidential information displayed
Under no circumstances should, PID, SID or confidential information be stored on portable devices such as pen drives, lap tops, CD's or Iphones
Access to patient information systems is restricted and individual passwords are required
PID and SID is not stored on the shared drive folders unless password protected
Documents containing PID or SID can be stored on the shared drive/departmental folders are password protected and version controlled
Rationale
Security of electronic records is maintained.

EAST LANCASHIRE HOSPICE
Standard Operating Procedure

Ensuring Accuracy And Quality Of Data

1. Overview

1.1 Information quality and records management are key elements of the information governance agenda. The information quality and records management assurance framework should be supported by adequate skills, knowledge and experience around health records, care records and corporate records, across the whole organisation. The levels of competency should be commensurate with the duties and responsibilities of particular posts or staff groups to provide an adequate level of assurance.

2. Process

2.1 Information Quality

Process
Clinicians are responsible for the quality of their record keeping in line with guidance from professional bodies
Service Managers and Heads of Department are responsible for monitoring the information quality produced in their services/departments incorporating data quality, and the correction of errors
Records should be factual, accurate, clear, legible and contemporaneous. Paper records are in black ink
Abbreviations and jargon are avoided
Any alterations to paper records are made by scoring through an entry with a single pen line so the original record can be read and the alteration dated and signed
Any alterations to electronic records are tracked and named as a new version with the date and initials of the individual making the alteration
All entries in paper records are signed and dated
All electronic documents are named and version controlled according to the following naming convention Title of the document, initial of creator, date it was created, Version (draft Version 1,2 etc), e.g **Brief guide to filing electronic documents DW10.12.15 Draft1**
All documents should be consistent in format according to guidance in the Written Information Policy and be written in plain English with good spelling and grammar
All corporate documents and templates are approved via a Governance Committee or the Senior management Team
Rationale
• Information quality is achieved.

2.2 Health Records

Process
For health and social care, the primary reason for managing information and records is for the provision of high quality care.
Professional staff must apply professional codes produced by their professional body in regard to health and social care record keeping to all health records
All medical records, both paper and electronic, have an NHS Number stored on them as early as possible in the episode of care. Staff routinely use the NHS Number as part of the provision of care, to link the service user to their health/care record, to communicate within and between organisations and ensure service user awareness of the NHS Number.
The patient’s complete medical record should be available at all times during their stay in the hospice. records from NHS are requested and tracked -using the PAS system via Clinical Administration

Every page in the medical record should include the patient's name, NHS number & may include local ID and the name of the hospice
The contents of the hospice record have a standardised structure and layout that must be followed and maintained, it should reflect the continuum of patient care and should be viewable in chronological order. Electronic EMIS record reads from most current entry to the most historic entry – like reading a book backwards
Every entry in the hospice record should be dated, timed (24 hour clock), legible and signed by the person making the entry. The name and designation of the person making the entry should be legibly printed against their signature. Deletions and alterations should be countersigned, dated and timed
Entries to the hospice record should be made as soon as possible after the event to be documented (for example change in clinical presentation, ward round, investigation) and before the relevant staff member goes off duty. If there is a delay, the time of the event and the delay should be recorded
Every entry in a Hospice record should identify the most senior healthcare professional present (who is responsible for decision making) at the time the entry is made
An entry should be made in hospice record whenever a patient is seen by a doctor. When there is no entry in the record for more than four (4) days the next entry should explain why
Advanced Decisions to Refuse Treatment, Consent, and Cardiopulmonary Resuscitation decisions must be clearly recorded in the Hospice record. In circumstances where the patient is not the decision maker, that person should be identified e.g. Lasting Power of Attorney
Allergens should be clearly highlighted and be immediately visible
Rationale
• Professional codes regarding record keeping are adhered to • Provide access to documentation at all times as team has access to all files • To maintain quality of medical records • Reduce delays in medical records being made available to medical staff. • Compliance with - AoMRC medical record keeping standards

Disclosure, Sharing And Transfer Of Personal Data

1. Overview

1.1 The organisation ensures that arrangements are in place to support and promote information sharing for coordinated and integrated care, and staff are provided with clear guidance on sharing information for care in an effective, secure and safe manner.

1.2 All organisations have a legal duty to keep all personal information secure and to respect confidentiality when personal information is held in confidence. The obligation to keep personal information secure and to respect confidentiality stems from common law, data protection and human rights legislation and applies to all organisations.

1.3 Staff working for and on behalf of the organisation must also meet these legal requirements and may be bound by professional obligations, employment contracts or other contractual measures.

1.4 Information about service users should be disclosed or transferred following the Caldicott principles detailed below:

- Principle 1: Justify the purpose for using the information
- Principle 2: Only use identifiable information if absolutely necessary
- Principle 3: Use the minimum that is required
- Principle 4: Access should be on a strict need to know basis
- Principle 5: Everyone must understand their responsibilities
- Principle 6: Understand and comply with the law
- Principle 7: The duty to share information can be as important as the duty to protect patient confidentiality.

1.5 Data subjects have the right to data portability

2. Procedure

2.1 Objections to Information Disclosure or Sharing (Patient Records)

Process
Any objection to disclosure or information sharing is dealt with by the most senior professional delivering care to that individual
The individual is advised of the implications their objection could have on the effectiveness of their care, how it may negatively impact on their care
The senior person caring for the patient considers if there is demonstrable risk that the safety of the patient will be reduced by not upholding the objection
The Caldicott Guardian is informed of all such objections and will consider if there are any compelling legitimate grounds relating to the individual’s situation
Rationale
Compliance with Caldicott 2.

2.2 Disclosure Requirements

Process
Sharing of information is on a strictly need to know basis with the explicit consent of the individual whom the information relates to for a specified purpose
Individuals have the right to request that information about them is withheld from another person or agency. These wishes are respected unless the following exceptional circumstances apply: • The disclosure is authorised by statute of law • There is an overriding public interest such as crime prevention or safeguarding

Consent is obtained from those whose information or images are displayed in publicity material on the website, social media or in hard copy newsletters , posters etc
Rationale
• Consent obtained for disclosure of information • Individuals wishes regarding disclosure respected unless in exceptional circumstances in line with legislation.

2.3 Disclosure Without Consent

Process
If the person is unable to consent to disclosure it will only take place in their best interests
Disclosure without consent is authorised when: • The disclosure is authorised by statute of law • There is an overriding public interest such as crime prevention or safeguarding
Where information is to be disclosed about a patient without or against their consent, the decision to release information rests with the Caldicott Guardian who will make a case by case judgement based on Caldicott principles
Where information is to be disclosed about a member of staff, volunteer, student or contractor without or against their consent of the individual the decision to release information rests with the Information Governance Lead who will make a case by case judgement based on legal principles
Information that has been anonymised/pseudonyms used or redacted can be shared for justified purposes as long as there is no Personal Identifiable Information
Rationale
• Compliance with legislation and best practice guidance • Decision to disclose made by individual with relevant knowledge, skills and responsibility.

2.4 General Requirements for Transfer of Information

Process
Individuals should be aware that information about them is to be transferred and be in agreement with the transfer
Information must only be transferred to a known recipient with authorisation to receive the information
Information should be transferred swiftly and securely to support provision of care or achievement of business objectives
The security of any transferred information should be maintained during transit up to the point of receipt
Rationale
• Consent to transfer information obtained • Minimise risk of unauthorised disclosure • Ensure care provision is maintained • Security maintained throughout transfer of information.

2.5 Requests for Information Made by Third Parties

Process
Information should not be disclosed or shared with anyone whose identification cannot be validated
Requests for information by the police should be in writing (S29 Certificate) stating what information is required, why they require it, and it must be signed by a senior officer. These requests should be referred to the Information Governance Lead or Caldicott Guardian
Requests for information from the media should be referred to the CEO or Fundraising Services Manager
Rationale
• Minimises risk of disclosure to unauthorised individuals • Compliance with legislation and best practice guidance • Decision to disclose made by individual with relevant knowledge, skills and responsibility • Appropriate information provided to media reducing risk of reputational damage.

2.6 Transfer of Information by Telephone

Process
When making a phone call; to a patient, family member, member of staff or volunteer do not leave personal information on answer services. Simply state your name contact number and request the person call you back
When asked for information over the telephone verify the identity of the person you are speaking to
Rationale
• Minimises risk of transfer to unauthorised individuals.

2.7 Transfer of Information by Post

Process
All correspondence containing Personal Identifiable Information or Sensitive Personal Information should be in a sealed envelope addressed to a named recipient and marked private and confidential. Windowed envelopes should not be used
Case notes should be sent via Clinical Administration. They are placed in a securely sealed polythene envelope (polylopes) and the address of the recipient should be clearly marked
Case notes should only be transferred via internal mail and return of case notes to East Lancashire Acute Hospitals NHS trust are be tracked on the PAS system by the Clinical Administration team.
Clinical administration should be advised of any case notes transferred into the hospital with a patient at the earliest opportunity so the notes can be effectively tracked via PAS
Rationale
• Minimises risk of transfer to unauthorised individuals • Track transfer of case notes.

2.8 Transfer of Information via Fax

Process
Minimum personal identifiable information should be sent by fax
The date and time on fax machines is checked each week by the Clinical Administration team and a record made in the log
Personal information and sensitive personal information should only be sent to designated safe haven faxes or to named recipients
Before transmitting information via fax the sender should complete the fax header form and document that: • The recipient’s identity and fax number have been confirmed prior to transmission by telephone • The receipt of the fax in its entirety has been confirmed with the recipient by telephone
Rationale
• Minimises risk of unauthorised disclosure • Ensure fax machines display correct date and time • Minimises risk of transfer to unauthorised individuals.

2.9 Transfer of Information via Email

Process
Minimum personal identifiable information should be sent by email
Documents with personal identifiable information should be password protected at all times and the recipient provided with the password via telephone or separate email once identity established and email address checked
Emails should be sent via NHS net accounts (Net to Net) when transferring patient information with PID or SID being attached and password protected rather than in the main body of the email. Details of secure emails across the health economy can be found in the resource section of this policy
Rationale
• Minimises risk of unauthorised disclosure • Minimises risk of transfer to unauthorised individuals.

2.10 Sharing Correspondence with Patients

Process
All service users are offered the opportunity to be copied into correspondence about their care at initial assessment and are informed about with whom their information is shared
The clinician will establish the patient's wishes for copies of correspondence on assessment and at review communicating this to the Clinical Administration Team
The Clinical Administration Team will copy correspondence to those patients who have accepted this offer, recording this on the bottom of each letter
Rationale
Service users know what information is shared with whom and consent to this.

2.11 Abuse of Privileges

Process
It is strictly forbidden for hospice employees, volunteers, students or contractors to access or request others information without appropriate authority. This includes accessing information relating to their own family or friends unless they are directly involved in the patient's care or their role requires them to access records on behalf of the hospice
Staff, volunteers, students and contractors should not talk about the hospice, it's business or personal information regarding patients, staff or volunteers in public places where they may be overheard
Staff, volunteers, students and contractors should not post personal information regarding patients, staff or volunteers on social media unless consent has been obtained to promote official hospice fundraising and marketing events
Abuse of privileges will be dealt with under the performance management procedures
Rationale
Behaviour that constitutes an abuse of privileges and the consequences are known by all.

2.12 Sharing/Transfer of Health Records

Process
The hospice has information sharing agreements with local CCG's EL~~A~~HT and other hospices in East Lancashire to enable sharing of information with other professionals involved in provision of health care to hospice patients
The IG Lead has copies of all information sharing agreements for IG toolkit evidence
The Clinical Services Manager ensures information is shared as per agreements in place to support patient care
Rationale
Compliance with best practice Ensure sharing of information to support patient care

2.13 Data Portability

Process
All requests for data portability must be sent to the Information Governance Lead who will work with the relevant Information Asset Owner to respond
A response to a request will be made within 1 month of receipt; this can be extended by two months where the request is complex or where a number of requests are received. The individual will be informed within one month of the receipt of the request and explain why the extension is necessary
The right to data portability only applies to personal data an individual has provided to a controller; where the processing is based on the individual's consent or for the performance of a contract; and when processing is carried out by automated means
The personal data will be provided in a structured, commonly used and machine-readable form. Which means that the information is structured so that software can extract specific elements of the data. This enables other organisations to use the data.
The information will be provided free of charge
If the individual requests it, it may be required to transmit the data directly to another organisation if this is

technically feasible. However, we are not required to adopt or maintain processing systems that are technically compatible with other organisations
If the personal data concerns more than one individual, consideration will be given to whether providing the information would prejudice the rights of any other individual
Where the decision is made not to take action in response to a request, this will be explained to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month
Rationale
Centralised point of contact for dealing with data portability requests Compliance with legislation.

EAST LANCASHIRE HOSPICE
Standard Operating Procedure

Retention, Archiving and Destruction of Information

1. Overview

1.1 Records are retained for the appropriate period of time, archived securely and destroyed appropriately in line with legislation and information governance best practice guidance.

2. Procedure

2.1 Retention of Patient Records

Process
Records are kept for the **Minimum Retention Period unless subject to an Inquiry**
The following types of record are covered by the health care records retention schedule (regardless of the media on which they are held) including paper, electronic, images and sound • Patient health records (electronic or paper-based, and concerning all specialties, including GP medical records) • Records of private patients seen on NHS premises • Accident & Emergency, birth and all other registers • Theatre, minor operations and other related registers • X-ray and imaging reports, output and images • Photographs, slides and other images • Microform (ie microfiche/microfilm) audio and video tapes, cassettes, CD-ROMs, etc • Emails • Computerised records • Scanned documents
Retain all records for patients who have received an organ transplant for 11 years
Retain all records for all other patients over the age of 18 for 8 years
The minimum retention periods should be calculated from the beginning of the year after the last date on the record
When archiving medical records a sticker denoting the date of destruction as determined by the above criteria should be put on the front cover
EMIS system lock access to deceased patient records, with permissions for re-entry Where there has been no activity on the record for 8 years the hospice record will be deleted and a record made that deletion of that record has taken place. This will be facilitated via the HOCA who will check access date reports each year and delete accordingly
Rationale
Retention of patient records in compliance with best practice guidance.

2.2 Retention of Records Relating To Staff, Volunteers, Donors or Contractors

Process
Records are kept for the **Minimum Retention Period unless subject to an Inquiry**
Records relates to all information (regardless of the media on which they are held) including paper, electronic, images and sound
The IAO identifies the retention period for all information they are responsible for on the Information Asset Register
The IAO audits their service regularly to ensure retention periods are met

Rationale
Retention of records is controlled by the IAO and is compliant with best practice guidance.

2.3 Archiving Hard Copy Information

Process
There is a requirement to archive certain information for future reference when they are no longer in current use and when the retention period has not passed
When information is not required for current use the IAO arranges archiving of these documents in a suitable secure and accessible location
The information should be clearly labelled in a suitable file or envelope with: type of information, dates information relates from and to, date for destruction, and who the Information Asset Owner is
Access to archived information will be via request to the IAO
Rationale
• All archiving is carried out by the IAO who organises this with General Administration • Archived information labelled to ensure easy access • Security of archived information is maintained • Limited access to archived information.

2.4 Archiving Electronic Information

Process
There is a requirement to archive certain information for future reference when it is no longer required when the retention period has not passed
When information is not required for current use the IAO arranges archiving in a suitable format, in a secure drive
The information should be in an electronic folder clearly labelled Archive, type of information, dates information relates from and to, date for deletion and who the information owner is
Access to archived information will be via request to the IAO
Rationale
• All archiving is carried out by IAO who organises this with General Administration • Archived information labelled to ensure easy access • Security of archived information is maintained • Limited access to archived information.

2.5 Destruction of Hard Copy Information

Process
All hard copy documents containing Personal Identifiable Data or Sensitive Personal Data must be kept secure until destruction
Staff are responsible for placing office waste containing PID such as meeting papers, to do list, duplicate copies of information etc. in a black bin bag. This should be sealed and labelled with office waste for shredding, date and name of information owner. This will then be passed to General Administration shredding on pre- arranged dates when the shredding company attends the hospice
All hard copy corporate records and medical records are shredded after the period of retention has passed. The Head of Corporate Administration will go through archives and identify information for shredding together, with the Senior General Administrator double checking the contents of the box and that the retention period has expired
All documents for shredding will be decanted from a secure area to a secure shredding machine on site when the shredding company attend the hospice.
A record will be made by General Administration of the contents of each box prior to shredding including: document type dates from- to , retention period, date retention period expired, date shredded
The HOCA will keep shredding certificates on file.

Rationale

- Security of information maintained
- Staff take responsibility for shredding information they produce that contains PID or SPD
- Hard copy documents for shredding are double checked by two senior members of the administration team
- Records to be shredded are separated from records to be retained to prevent accidental shredding of documents still in the retention period
- Record made of what documents have been shredded
- Evidence secure destruction of hard copy documents.

2.6 Destruction of Electronic Records

Process

Information Asset Owners are responsible for ensuring the deletion of electronic information where it is no longer required and the archive period has passed . The Emis system does this automatically

The IAO will go through archived electronic folders with another member of their team, double checking the contents of the file and that the retention period has expired

A record will be made of the contents of each folder prior to deletion including: document type dates from- to, retention period, date retention period expired, date deleted.

Rationale

- Security of information maintained
- IAO take responsibility for deleting information they produce that contains PID or SPD
- Documents for deletion are double checked by two senior members of the administration team
- Able to track what documents have been deleted.

2.7 Erasure Of Personal Information At The Request Of The Data Subject

Process

Requests for erasure must be directed to the Information Governance Lead who will consider each on a case by case basis with the Information asset owner

Individuals have a right to have personal data erased and to prevent processing in specific circumstances:

- Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
- When the individual withdraws consent.
- When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
- If the personal data was unlawfully processed
- The personal data has to be erased in order to comply with a legal obligation.
- The personal data is processed in relation to the offer of information society services to a child.

A refusal to comply with a request for erasure can take place where the personal data is processed for the following reasons:

- To exercise the right of freedom of expression and information;
- To comply with a legal obligation or for the performance of a public interest task or exercise of official authority;
- For public health purposes in the public interest; archiving purposes in the public interest, scientific research historical research or statistical purposes;
- The exercise or defence of legal claims

If the personal data in question has been disclosed to third parties, they must be informed about the erasure of the personal data, unless it is impossible or involves disproportionate effort to do so.

Rationale

- Centralised approach to managing erasure requests
- Compliance with legislation

EAST LANCASHIRE HOSPICE
Standard Operating Procedure

Management Of Data Subject Access Requests

1. Overview

The reason for allowing individuals to access their personal data is so that they are aware of and can verify the lawfulness of the processing.

2. Procedure

2.1 Responding To Data Subject Access Request

Process
All individuals have the right to access their own information • Patients or their representatives can access their medical records via a written request to the Caldecott Guardian • Access to deceased patient's records can only be made by the deceased personal representative, usually the executor of the will, access will be considered taking into account the known wishes of the patient during life and potential harm that may result if released via a written request to the Caldecott Guardian • Staff can request access to their personnel files via their Service Manager • Volunteers can request access to their records via the relevant Service Manager • Contractors can request information via the lead Service Manager for that contract • Service Managers will liaise with the DSSM as Information Governance lead before sharing information • All other subject access requests must be directed to the DSSM as Information Governance lead
Individuals wishing to exercise their right of access should: • make a written application to the organisation holding the records • provide information as the organisation may require to sufficiently identify the individual;
The identity of the person making the request, must be verified using "reasonable means".
If the request is made electronically, the information will be provided in a commonly used electronic format
Where you process a large quantity of information about an individual, it is permissible to ask the individual to specify the information the request relates to
A copy of the information must be provided free of charge. However, a 'reasonable fee' can be charged when a request is manifestly unfounded or excessive, particularly if it is repetitive or for requests for further copies of the same information. The fee must be based on the administrative cost of providing the information
Information must be provided without delay and at the latest within one month of receipt. This can be extended by a further two months where requests are complex or numerous. If this is the case, the individual must be informed within one month of the receipt of the request and explain why the extension is necessary.
Where requests are manifestly unfounded or excessive, in particular because they are repetitive, you can: refuse to respond. Where you refuse to respond to a request, you must explain why to the individual, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month
All details of third parties in records will be redacted to protect their confidentiality
All decisions to provide access will consider the potential for harm from allowing or controlling access
The hospice is exempt from the Freedom of Information Act. Any requests for information will be considered by the Information Governance Lead, Caldecott Guardian and CEO on a case by case basis
Access to information encompasses the following rights to: • Obtain a copy of the record in permanent form; • Have information provided in an intelligible format (and explained where necessary, e.g. medical)
Where the individual agrees, the access right may be met by providing a facility for the individual to view the record without obtaining a copy

Access may be denied or restricted where:

- the record contains information which relates to or identifies a third party that is not a care professional and has not consented to the disclosure. If possible the individual should be provided with access to that part of the record which does not contain the third party information. Ideally, it should be explained to third parties' before they disclose any information that if an individual makes an access request, he/she may be able to identify the source of the information even if the identity of the third party is withheld.
- access to all or part of the record will prejudice the carrying out of social work by reason of the fact that serious harm to the physical or mental well-being of the individual or any other person is likely. If possible the individual should be provided with access to that part of the record that does not pose the risk of serious harm.

The individual has a right of appeal against a decision to refuse access to their information. They should contact the CEO in writing within 30 days of the decision being communicated to them. Individuals are also provided with the details of the Information Commissioners office from the ICO website at: https://www.ico.org.uk/Global/contact_us

Rationale

- Centralised point for considering and responding to data subject access requests
- Compliance with legislation.

EAST LANCASHIRE HOSPICE

Standard Operating Procedure

Information Governance Information, Training and Support

1. Overview

1.1 Information Governance awareness and mandatory training procedures are in place and all staff are appropriately trained. The information governance agenda, confidentiality and data protection framework is supported by staff and volunteers with relevant skills, knowledge and experience in relation to their roles which meet the organisation's assessed training needs.

2. Procedure

2.1 Information Available

Process
All staff, volunteers and contractors are aware of their responsibilities and what is required of them in regard to information governance as this is detailed in job and role descriptions, staff contracts, mandatory training and this policy and SOP's. Volunteers, students and contractors also sign a confidentiality agreement that sets out expectations. In addition professional staff are bound by professional codes of practice relating to confidentiality
Rationale
Ensure staff members, volunteers and contractors are effectively informed of what is required of them in terms of confidentiality.

2.2 Induction and Mandatory Training

Process
There is an information governance section in the mandatory training workbook issued to all new staff and volunteers on commencement and annually thereafter. This information governance section includes key principles of effective record keeping
New starters are also directed to the information governance policy on commencement
Volunteers, students and contractors working regularly on site sign a confidentiality agreement on commencement detailing key principles of information governance
Rationale
• All staff and volunteers receive training on information governance at an introductory level on commencement and annually thereafter in line with NHS Information Governance Training Toolkit • New staff are aware of where to find information regarding information governance compliance and are aware of the expectations relevant to their role • Expectations regarding information governance compliance are provided to staff, volunteers, students and contractors.

2.3 Specific Training for HOD

Process
Training needs relating to information governance compliance will be considered by the Senior Management Team in the annual Training Needs Analysis
All Service Managers will complete education on the responsibilities of the Information Asset Owners
The Caldicott Guardian will access education on Caldicott
The SIRO and Information Governance Lead will access education for SIRO's
Rationale
• Training needs with regard to information governance are reviewed and identified each year • Service Managers who are Information Asset Owners have the skills, knowledge and experience to protect data they are responsible for

- Caldicott Guardian has relevant skills, knowledge and experience to carry out their role
- SIRO/Information Governance Lead has relevant skills, knowledge and experience to carry out their role.

2.4 Advice Available

Process
All staff, volunteers and contractors can seek advice via the HOD, Service Manager, Caldicott Guardian and Information Governance Lead
Rationale
Ensure staff members, volunteers and contractors are effectively informed of what is required of them in terms of confidentiality.

EAST LANCASHIRE HOSPICE

Standard Operating Procedure

Contractual Arrangements Regarding Information Governance

1. Overview

1.1 All organisations need to ensure that work conducted by others on their behalf meet all the required information governance standards. Where this work involves access to information about identifiable individuals it is likely that organisations will be in breach of the law where appropriate requirements have not been specified in contracts and steps taken to ensure compliance with those requirements. Formal contractual arrangements that include compliance with information governance requirements, are in place with all contractors and support organisations that have access to the organisation's information or conduct any form of information processing on its behalf.

2. Procedure

2.1 Review of Existing Contracts

Process
All existing contracts and Service Level Agreements are reviewed annually to identify if the work contracted out involves access to information about identifiable individuals
The Service Manager responsible will ensure there is specific reference to Information Governance requirements when the contract or SLA involves the third party having access to information about identifiable individuals
The Information Governance Lead maintains a list of contractors who have access to personal identifiable information
Rationale
• Identify which contractors have access to Personal Identifiable Information • The type of information that is processed by which contractors is clearly documented.

2.2 Ensuring Information Governance Requirements Are Explicit in All Contracts and SLA

Process
When contracts or SLA are being developed the Service Manager responsible will ensure there is specific reference to information governance requirements when the contract or SLA involves the third party having access to information about identifiable individuals
Rationale
• Contractors aware that information governance requirements should be specified in the contract • All contracts specify information governance requirements.

EAST LANCASHIRE HOSPICE
Standard Operating Procedure

Audit and Managing Information Governance Risk

1. Overview

1.1 Organisations should ensure that access to confidential personal information is monitored and audited locally and in particular ensure that there are agreed procedures for investigating and reducing information governance risk.

2. Procedure

2.1 Monitoring and Auditing

Process
All HOD assess risks relating to information governance as part of the quarterly departmental risk assessment and an action plan devised to reduce any identified risks
IAO maintain their own Information Asset Register and an organisational information asset register is updated annually and reported via the governance structure
DPO will conduct an annual audit with the IAO of data with for which they are responsible for considering, fair processing, consent, quality of information, security, sharing, archiving, retention and destruction
Compliance with the NHS IG toolkit to level two is achieved each year
All risks identified are seen by the Information Governance Lead and reported to the Non- Clinical Governance Committee who monitor any action arising through to completion
Rationale
• IAO know what information is held in their service and review this at least annually • The organisation has an up to date Information Asset Register • Compliance with legislation, best practice and policy is audited annually by all IAO • Risks relating to information governance are pro-actively identified and action taken to reduce any risks found • Information governance practice is audited and reported at a senior level through the governance framework.

2.2 Managing Information Governance Risks

Process
All actual or potential information governance risks are reported and investigated in accordance with the Risk Reporting, Reducing and Review SOP of the Health Safety and Risk Management Policy
Complaints with elements relating to information governance are managed in accordance with the Complaints Policy and associated SOP
Any information governance risk will be reviewed by the Caldicott Guardian and Information Governance Lead
Serious incidents will be reported in accordance with SIRI's Guidance
Rationale
• Information governance risks are reported and reviewed by those with relevant leads and actions to reduce risk.

Considering Information Governance Implications For New Developments, Information Systems And Assets

1. Overview

1.1 All new processes, services, information systems, and other relevant information assets are developed and implemented in a secure and structured manner, and comply with information governance security accreditation, information quality and confidentiality and data protection requirements.

1.2 All organisations experience change in one form or another. Service redesign and rapidly changing technology has a major impact on processes and systems already in place, often requiring change simply to keep up to date and to enable the safe and secure processing of personal information.

1.3 It is vitally important that the impact of any proposed changes to the organisation's processes and/or information assets are assessed to ensure that the confidentiality, integrity and accessibility of personal information are maintained.

2. Procedure

2.1 Development of Information Governance Processes, Services and Information Assets

Process
Information governance considerations are embedded in the report template used to discuss and approve developments and initiatives via Governance and Senior Managers Meetings
The Information Governance Lead and Caldicott Guardian are members of Governance and Senior Managers Meetings where the design phase of any new service, process or information asset will be discussed and approved. They can highlight risks and advice if a privacy impact assessment is required for a particular project or plan
All IT systems that contain clinical information are developed and maintained via contract with NHS providers who are complaint with NHS toolkit
Each Service Manager keeps an Information Asset Register of the information they are responsible for - this feeds into the organisational Information Asset Register detailing the type of information, format it is kept in, location, access, rationale for keeping, retention period and any action required to improve information governance. This is reviewed annually
Training is provided to relevant staff on the effective and safe use of IT systems and user guides are also available
All IT systems and information are backed up under the IT Service level Agreement
Rationale
• Compliance with Legislation and best practice guidance.

EAST LANCASHIRE HOSPICE
Standard Operating Procedure

Payment Card Industry Data Security Standard (PCI DSS) Compliance

1. Overview

1.1 The Hospice handles sensitive cardholder information daily and are used in Retail, Fundraising and Finance Services. Sensitive Information must have adequate safeguards in place to protect the cardholder data, cardholder privacy, and to ensure compliance with various regulations, along with guarding the future of the organisation.

1.2 PCI DSS is a set of comprehensive and universal security standards for all organisations handling cardholder data. Consumers are increasingly aware not only of the existence of PCI DSS but also of the protection it gives them when shopping online or providing their card details over the telephone.

1.3 There are twelve specific requirements and procedures for attaining PCI DSS compliance and these are split across six areas as follows: - Build and maintain a secure network, protect cardholder data, maintain a vulnerability management program, implement strong access control measures, regularly monitor and test networks, and maintain an Information Security policy.

2. Procedure: System security

2.1 Maintain a Firewall Configuration to Protect Cardholder Data

Process	Rationale
East Lancashire Hospice outsources the secure network and system configuration and in doing so ensures that the service provider has systems in place for firewall configuration and to detect firewall changes	Provide a secure pathway for those making payments by the ELH card machine and via the website
Firewalls restrict connections between untrusted networks and any system in the cardholder data environment	Compliance with PCI requirement 1.2
Firewalls prohibit public access between the internet and any system component in the cardholder data environment	Compliance with PCI requirement 1.3.

2.2 Vendor-Supplied Defaults for System Passwords Not to Be Used

Process	Rationale
Vendor-supplied defaults are always changed before a system is installed on the network by IT services	Compliance PCI requirement 2.1
Defaults for wireless systems are changed before implementation by specified staff user	PCI requirement 2.1.1

2.3 High Level network diagram

Process	Rationale
A high-level network diagram of the network is maintained and reviewed on a yearly basis. The network diagram provides a high level overview of the cardholder data environment (CDE), which at a minimum shows the connections in and out of the CDE. Critical system components within the CDE, such as POS devices, databases, web servers, etc., and	Connections to CDE are known and updated

any other necessary payment components, as applicable should also be illustrated	

2.4 Use and Regularly Update Anti-Virus Software or Programs

Process	Rationale
East Lancashire Hospice outsources the anti-virus software and program updates and in doing so must ensure that the service provider has systems in place for anti-virus installation on personal computers and servers, the anti-virus software must be completely up to date and capable of detecting, removing and protecting against all known types of malicious software	PCI requirement 5.1 and 5.1.1
The anti-virus programs used by outsourced service providers must be kept current, be actively running, and capable of generating audit logs	PCI requirement 5.2

2.5 Develop and Maintain Secure Systems and Applications

Process	Rationale
All critical security patches must be installed within one month of release and updates must be received on a regular basis. IT updates in regard to Server, Raisers Edge via blackboard and Stirling for lottery system,	PCI requirement 6.1

2.6 Encrypt Transmission of Cardholder Data Across Open, Public Networks

Process	Rationale
Sending unencrypted PANs by end-user messaging technologies is prohibited (e.g. email, instant messaging and chat).Cardholder data sent across open, public networks must be protected through the use of strong cryptography or security protocols- No card holder data is sent via emails, only access is by secure payment gateways of PCI compliant organisations	PCI requirement 4.1 PCI requirement 4.2

2.7 Assign a Unique ID to Each Person with Computer Access

Process	Rationale
East Lancashire Hospice employees have a username and unique password to login to their personal computer and when the PC is not in use staff must lock their computer screen	PCI requirement 8 Refer to Information Governance Policy legal requirements
IAO authorises access to systems and individual generates own password	
All accounts used by outsourced service providers for remote maintenance are enabled only during the time period needed. At all other times these accounts must be disabled. Access authorised by individual with access to system reporting the fault	PCI requirement 8.5.6

2.8 Track and Monitor All Access to Networks Resources and Cardholder Data

Process	Rationale
East Lancashire Hospice outsources the monitoring of access to the hospice network and in doing so must ensure that the service provider has systems in place to	PCI requirement 10

perform regular (at least quarterly) testing of staff and volunteer network access permissions.	

2.9 Regularly Test Security Systems and Processes

Process	Rationale
East Lancashire Hospice outsources the vulnerability scanning and testing for unauthorised wireless access points to MLCSU and in doing so must ensure that the service provider has systems in place to perform regular (at least quarterly) testing	PCI requirements 11.1 and 11.2

2.10 Recording and monitoring compliance

Process	Rationale
Maintain a list of services providers See IAR	PCI requirement 12.8.1
Maintain written agreements that include an acknowledgement that the service providers are responsible for the security of the cardholder data the service provider possess – detailed in IAR	PCI requirement 12.8.2
Perform proper due diligence prior to engaging a service provider, ensuring a copy of their policy is obtained and checked by East Lancashire Hospice Information Governance Lead	PCI requirement 12.8.3
Monitor service providers PCI DSS compliance status on an annual basis upon the expiry date of the service providers PCI Compliance Certificate- Via FSM	PCI requirement 12.8.4
Monitor East Lancashire Hospice PCI DSS compliance on an annual basis upon the expiry date of the hospices PCI Compliance Certificate via FSM	

3. Protecting card holder information

3.1 Restrict Physical Access to Cardholder Data

Process	Rationale
Access to East Lancashire Hospices cardholder data is limited to only those individuals whose job requires such access	PCI requirement 7.1
Access to cardholder data is based on an individual's job classification and function. Access to cardholder data must be granted by management who will authorise staff user names, login details and passwords in order to access the cardholder data	PCI requirement 7.1
Printed reports containing cardholder data are to be physically retained, stored or archived only within secure East Lancashire Hospice office environments, and only for the minimum time deemed necessary for their use. All cardholder data is shredded using a cross cut shredder after the payment has been processed and once all returned card payments have been dealt with and after all month-end procedures are complete	PCI requirement 9.6 PCI requirements 9.10 and 9.10.1 To ensure the cardholder data cannot be reconstructed
All hardcopy media containing cardholder data is stored in a secure and locked container (e.g. cabinet or	PCI requirement 9.6

desk drawer is fine) and should never be left unattended in open workspaces	
At no time is printed material containing cardholder data to be removed from any East Lancashire Hospice office, storage area or retail outlet without prior written authorisation from a senior manager and all confidential or sensitive hardcopy material is not or delivered outside the organisation	PCI requirement 9.8 PCI requirement 9.7.2

3.2 Protect Cardholder Data

Process	Rationale
Employees handling sensitive cardholder data should ensure they: ● Handle Company and cardholder information in a manner that fits with their sensitivity and classification in order to protect sensitive cardholder information; ● Keep passwords and accounts secure; ● Request approval from management prior to establishing any new software or hardware, third party connections, etc.; ● Always leave desks clear of sensitive cardholder data and lock computer screens when unattended; ● Hospice employees must not write down card details on paper, nor should donors card details be stored electronically, this includes email accounts	Card holder information secure
Sensitive authorisation data (e.g. CVC card verification codes, PIN personal identification number and the full contents of any track from the magnetic stripe located on the back of a card) should be retained only until completion of the authorisation of a transaction. Storage of sensitive authorisation data post-authorisation is forbidden	PCI requirements 3.2.1, 3.2.2 and 3.2.3
East Lancashire Hospice masks the display of PANs (primary account numbers), and limit viewing of PANs to only those employees and other parties with a legitimate need. A properly masked number will show only the last four digits of the PAN	PCI requirement 3.3
Employees shall not use or otherwise employ employee-facing technologies to store, process or otherwise handle cardholder data. Employee-facing technologies include remote-access technologies, wireless technologies, removable electronic media, laptops, personal data/digital assistants (PDAs), email and internet usage	PCI requirement 12.3
An automatic process must exist to permanently delete on-line data, when no longer required All cardholder data on electronic media must be rendered unrecoverable when deleted e.g. through degaussing or electronically wiped using military grade secure deletion processes or the physical	

destruction of the media; If secure wipe programs are used, the process must define the industry accepted standards followed for secure deletion	

4. Credit Card Incident Response

Process	Rationale
The Hospice PCI Security Incident Response Team (PCI Response Team) is comprised of the CEO, DPO and the Finance Services security incident response plan is as follows: Each department must report an incident to via the risk reporting form as soon as a risk is identified The DSSM- will advise the PCI Response Team of the incident on receipt of the report. The PCI Response Team will investigate the incident and assist the potentially compromised department in emitting the exposure of cardholder data and in mitigating the risks associated with the incident. The PCI Response Team will resolve the problem to the satisfaction of all parties involved, including reporting the incident and findings to the appropriate parties (credit card associations, credit card processors, etc.) as necessary. The PCI Response Team will determine if policies and processes need to be updated to avoid a similar incident in the future, and whether additional safeguards are required in the environment where the incident occurred, or for the institution.	Risks are responded to promptly and appropriately
In response to a systems compromise, the PCI Response Team will laisse with MLCSU or the system provider to: Ensure compromised system/s is isolated on/from the network. Gather, review and analyse the logs and related information from various central and local safeguards and security controls Conduct appropriate forensic analysis of compromised system. Contact internal and external departments and entities	

as appropriate. Make forensic and log analysis available to appropriate law enforcement or card industry security personnel, as required. Assist law enforcement and card industry security personnel in investigative processes, including in prosecutions	
The credit card companies have individually specific requirements that the Response Team must address in reporting suspected or confirmed breaches of cardholder data. See appendix XX for these requirements	

Appendix

Incident Response notifications to various card schemes

VISA Steps

If the data security compromise involves credit card account numbers, implement the following procedure:

- Shut down any systems or processes involved in the breach to limit the extent, and prevent further exposure.
- Alert all affected parties and authorities such as the Merchant Bank (your Bank), Visa Fraud Control, and the law enforcement.
- Provide details of all compromised or potentially compromised card numbers to Visa Fraud Control within 24 hrs.
- For more Information visit: http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_if_compromised.html

Visa Incident Report Template

This report must be provided to VISA within 14 days after initial report of incident to VISA. The following report content and standards must be followed when completing the incident report. Incident report must be securely distributed to VISA and Merchant Bank. Visa will classify the report as "VISA Secret"*.

I. Executive Summary
    - Include overview of the incident
    - Include RISK Level(High, Medium, Low)
    - Determine if compromise has been contained

II. Background

III. Initial Analysis

IV. Investigative Procedures

I. Include forensic tools used during investigation

V. Findings

- Number of accounts at risk, identify those stores and compromised
- Type of account information at risk
- Identify ALL systems analysed. Include the following:
    - Domain Name System (DNS) names
    - Internet Protocol (IP) addresses
    - Operating System (OS) version
    - Function of system(s)
- Identify ALL compromised systems. Include the following:
    - DNS names
    - IP addresses
    - OS version
    - Function of System(s)

VI. Timeframe of compromise
    - Any data exported by intruder
    - Establish how and source of compromise
    - Check all potential database locations to ensure that no CVV2, Track 1 or Track 2 data is stored anywhere, whether encrypted or unencrypted (e.g., duplicate or backup tables or databases, databases used in development, stage or testing environments, data on software engineers' machines, etc.)
    - If applicable, review VisaNet endpoint security and determine risk

VII. Compromised Entity Action
VIII. Recommendations
IX. Contact(s) at entity and security assessor performing investigation

*This classification applies to the most sensitive business information, which is intended for use within VISA. Its unauthorized disclosure could seriously and adversely impact VISA, its employees, member banks, business partners, and/or the Brand.

MasterCard Steps:

- Within 24 hours of an account compromise event, notify the MasterCard Compromised Account Team via phone at 1-636-722-4100.
- Provide a detailed written statement of fact about the account compromise (including the contributing circumstances) via secured e-mail to compromised_account_team@mastercard.com.
- Provide the MasterCard Merchant Fraud Control Department with a complete list of all known compromised account numbers.
- Within 72 hours of knowledge of a suspected account compromise, engage the services of a data security firm acceptable to MasterCard to assess the vulnerability of the compromised data and related systems (such as a detailed forensics evaluation).
- Provide weekly written status reports to MasterCard, addressing open questions and issues until the audit is complete to the satisfaction of MasterCard.
- Promptly furnish updated lists of potential or known compromised account numbers, additional documentation, and other information that MasterCard may request.
- Provide finding of all audits and investigations to the MasterCard Merchant Fraud Control department within the required time frame and continue to address any outstanding exposure or recommendation until resolved to the satisfaction of MasterCard.

Once MasterCard obtains the details of the account data compromise and the list of compromised account numbers, MasterCard will:

- Identify the issuers of the accounts that were suspected to have been compromised and group all known accounts under the respective parent member IDs.
- Distribute the account number data to its respective issuers.

Employees of the company will be expected to report to the security officer for any security related issues. The role of the security officer is to effectively communicate all security policies and procedures to employees within the company and contractors. In addition to this, the security officer will oversee the scheduling of security training sessions, monitor and enforce the security policies outlined in both this document and at the training sessions and finally, oversee the implantation of the incident response plan in the event of a sensitive data compromise.

Discover Card Steps

- Within 24 hours of an account compromise event, notify Discover Fraud Prevention at (800) 347-3102
- Prepare a detailed written statement of fact about the account compromise including the contributing circumstances
- Prepare a list of all known compromised account numbers
- Obtain additional specific requirements from Discover Card

American Express Steps

- Within 24 hours of an account compromise event, notify American Express Merchant Services at (800) 528-5200 in the U.S.
- Prepare a detailed written statement of fact about the account compromise including the contributing circumstances
- Prepare a list of all known compromised account numbers Obtain additional specific requirements from American Express

Appendix 1: Information Governance Management Frame work

INFORMATION GOVERNANCE MANAGEMENT FRAMEWORK		
Heading	**Requirement**	**Notes**
Senior Roles	Information Governance Lead Senior Information Risk Owner (SIRO) Caldecott Guardian	The Information Governance lead is the Development and Support Services Manager The SIRO is the Development and Support Services Manager The Caldecott Guardian Is the Clinical Services Manager
Key Policies	Over-arching Information Governance Policy Data Protection Act 1998/Confidentiality Policy Organisation Security Policy Information Lifecycle Management Policy Corporate Governance Policy	There is an overarching Information Governance Policy Data protection and confidentiality is included in the Information Governance policy and associated SOP Handling information Securely is an SOP of the Information Governance policy SOP's are in place for the lifecycle of information management There is a corporate governance policy
Key Governance Bodies	Information Governance Board/Forum/Steering Group	The Information Governance agenda is a standing agenda item on the Non- Clinical Governance Committee Agenda and is feedback to Board in quarterly reports
Resources	Details of key staff roles and dedicated budgets	IT contract provided by Lancashire and Midlands CSU under a SLA Role descriptions and policy details Information Governance responsibilities

Heading	Requirement	Notes
Governance Framework	Details of how responsibility and accountability for Information Governance is cascaded through the organisation.	Responsibility with regard to Information Governance is included in specific Job Descriptions for the Information Governance Lead, SIRO and the Caldecott Guardian Responsibilities are detailed on the Information Governance policies and associated SOP Staff responsibilities regarding Information Governance are detailed in contracts and Job Descriptions Volunteer responsibilities are detailed in Role descriptions and volunteers are required to sign a declaration of confidentiality on commencement Cleaning contractors are required to sign a declaration of confidentiality on commencement Contactors are advised of Information Governance in line with the access to information they have under the contract/ SLA
Training & Guidance	Staff Code of Conduct Training for all staff Training for specialist Information Governance roles	All staff and volunteers complete mandatory training work books on commencement which includes a section on Information Governance, that mirrors content of the NHS Information Governance Training Tool Caldecott Lead accesses information and education relevant to the role Information Governance Lead accesses information and education relevant to the role Training Needs Analysis and PDR to identify training requirements of IAO with regard to Information Governance
Incident Management **(see requirements 307, 301 & 302)**	Documented procedures and staff awareness	There is clear guidance on incident management procedures documented in Information Governance Policy which is detailed in the mandatory training work book. Additional taught sessions on risk reporting, reviewing and reduction are available for HOD , Service Managers and Team Leaders

Appendix 2

Data Subject Rights

The Right to Be Informed

The right to be informed encompasses the organisations obligation to provide 'fair processing information', typically through a privacy notice. It emphasises the need for transparency over how you use personal data.

What Information Must Be Supplied?

The GDPR sets out the information that should be supplied and when individuals should be informed. The information required is determined by whether or not you obtained the personal data directly from individuals. See the table below for further information on this. The information you supply about the processing of personal data must be concise, transparent, intelligible and easily accessible; written in clear and plain language, particularly if addressed to a child; and free of charge.

Information required	Obtained directly from the data subject	Obtained indirectly
Identity and contact details of the data controller and the data protection officer	YES	YES
Purpose of the processing and the lawful basis for the processing	YES	YES
The legitimate interests of the data controller or third party, where applicable	YES	YES
Categories of personal data	NO	YES
Any recipient or categories of recipients of the personal data	YES	YES
Details of transfers to third country and safeguards	YES	YES
Retention period or criteria used to determine the retention period	YES	YES
The existence of each of data subject's rights	YES	YES
The right to withdraw consent at any time, where relevant	YES	YES
The right to lodge a complaint with a supervisory authority	YES	YES
The source the personal data originates from and whether it came from publicly accessible sources	NO	YES
Whether the provision of personal data is part of a statutory or contractual requirement or obligation and possible consequences of failing to provide the personal data	YES	NO
The existence of automated decision making, including profiling and information about how decisions are made, the significance and the consequences.	YES	YES

When is the information required	Obtained directly from the data subject	Obtained indirectly
	At the time the data are obtained.	Within a reasonable period of having obtained the data (within one month) If the data are used to communicate with the individual, at the latest, when the first communication takes place; or If disclosure to another recipient is envisaged, at the latest, before the data are disclosed

The Right of Access

Individuals have the right to obtain: confirmation that their data is being processed; access to their personal data; and other supplementary information – this largely corresponds to the information that should be provided in a privacy notice- see data subject access requests SOP

The Right to Rectification

Individuals are entitled to have personal data rectified if it is inaccurate or incomplete.
If you have disclosed the personal data in question to third parties, you must inform them of the rectification where possible. You must also inform the individuals about the third parties to whom the data has been disclosed where appropriate

The Right to Erasure

The right to erasure is also known as 'the right to be forgotten'. The broad principle underpinning this right is to enable an individual to request the deletion or removal of personal data where there is no compelling reason for its continued processing.

The Right to Restrict Processing

Individuals have a right to 'block' or suppress processing of personal data. When processing is restricted, the organisation is permitted to store the personal data, but not further process it. They can retain just enough information about the individual to ensure that the restriction is respected in future.

The Right to Data Portability

The right to data portability allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.

The Right to Object

Individuals have the right to object to: processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling); direct marketing (including profiling); and processing for purposes of scientific/historical research and statistics.

Rights Related To Automated Decision Making and Profiling

The legislation provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention. The hospice does not use any processing that constitute automated decision making.