East Suffolk and North Essex NHS Foundation Trust

Data Protection Policy

Version 2.0

Purpose:	• Documents the Trust's responsibilities in relation to the Data Protection Act and related Acts. • Provide clarity regarding the roles and responsibilities of all members of the Trust in relation to protection of person-identifiable information. • Provide guidance to staff regarding confidentiality issues in the form of a Code of Conduct. • Provide guidance to minimise the risk of breaching the Data Protection Act.
For use by:	• All members of Trust staff, including contractors, temporary staff, bank registrants, volunteers, students and pre-registration students • Community sites that come under the remit of East Suffolk and North Essex NHS Foundation Trust
This document is compliant with / supports compliance with:	• National Data Guardian Review 2016 • Data Protection Act 2018 • NHS Confidentiality Code of Practice 2003 • Access to Health Records Act 1990 • Computer Misuse Act 1990 • Freedom of Information Act 2000 • Human Rights Act 1998 • Common Law Duty of Confidence • NHS Digital Data Security & protection Toolkit
This document supersedes:	Data Protection Policy v1.0 (ESNEFT)
Approved by:	Information & Records Governance Group
Approval date:	10 October 2019
Implementation date:	10 October 2019
Review date	10 October 2022
In case of queries contact: Responsible Officer	Data Protection Officer
Directorate and Department	Information Governance
Archive Date i.e. date document no longer in force	*To be inserted by Information Governance Department when this document is superseded. This will be the same date as the implementation date of the new document.*
Date document to be destroyed: i.e. 10 years after archive date	*To be inserted Information Governance Department when this document is superseded*

Version and document control:

Version ID	Date of Issue	Change Description	Author
V1.0	May 2018	Reviewed as part of new General Data Protection Regulations and replaces Colchester and Ipswich policies	Head of Information Governance
2.0	September 2019	Annual Review	Information Governance Lead /Data Protection Officer

This is a Controlled Document

Printed copies of this document may not be up to date. Please check the hospital intranet for the latest version and destroy all previous versions.

Hospital documents may be disclosed as required by the Freedom of Information Act 2000.

Sharing this document with third parties
As part of the Trust's networking arrangements and sharing best practice, the Trust supports the practice of sharing documents with other organisations. However, where the Trust holds copyright to a document, the document or part thereof so shared must not be used by any third party for its own commercial gain unless this Trust has given its express permission and is entitled to charge a fee.

Release of any strategy, policy, procedure, guideline or other such material must be agreed with the Lead Director or Deputy/Associate Director (for Trust -wide issues) or Business Unit/ Departmental Management Team (for Business Unit or Departmental specific issues). Any requests to share this document must be directed in the first instance to the Data Protection Officer.

For further advice see the Development and Management of Trust wide Procedural Documents Policy

Contents

SECTION 1 - INTRODUCTION

1.1 Policy Statement and Rationale

As a prerequisite for complying with legislation and NHS Digital standards, this document sets out the hospital's policy and procedures to be followed in relation to data protection. This policy relates to all personal data held by the Trust relating to patients and employees.

The overall objective is to ensure that there is a hospital-wide approach to the management and implementation of data protection procedures, which is communicated to and available to all staff.

1.2 Key Principles

- All staff will ensure any person identifiable data they process as part of their role, including patients and employee data, will be in accordance with the General Data Protection Regulations (GDPR) which came into effect on 25 May 2018
- All staff must complete Information Governance training every year.
- If a new process involving the use of person-identifiable information is introduced, the Information Governance Team must be informed in order to check its compliance with GDPR
- The IG Team must be advised of the existence of any Information Asset.
- Staff are to ensure any contracts with third parties involving the processing of person identifiable data comply with the GDPR Contracts Protocol
- Only authorised staff should have access to person identifiable information for legitimate work purposes. Access for personal purposes is a disciplinary offence
- Computer systems processing patient identifiable data are auditable
- All confidentiality or data security breaches must be reported via Datix.
- The Information Governance Team will answer all queries on Data Protection and confidentiality issues in the first instance.
- The Information & Records Governance Group, chaired by the Caldicott Guardian, has overall responsibility for Data Protection and confidentiality matters at the Trust.

1.3 Background Information

The General Data Protection Regulation came into force on 25 May 2018. It unified the rights of EU member states and forms part of the Data Protection Act 2018. It replaces the Data Protection Act 1998.

The Data Protection Act 2018 is the UK's implementation of the GDPR and therefore this legislation will still apply once the UK leaves the EU.
Under the Data Protection (Charges and Information) Regulations 2018, the Trust is obliged by law to register all processing activities with the Information Commissioner's Office on an annual basis and failure to comply with this requirement is a criminal offence.

It is the policy of the Trust that the six principles underpinning the GDPR are fulfilled. The six Principles state that personal data shall be:

1. Processed fairly and lawfully
2. Collected for a specific, explicit and legitimate purpose, and shall not be further processed in a manner incompatible with those purposes
3. Adequate, relevant and necessary in relation to those purposes.
4. Accurate and where necessary kept updated
5. Not be kept for longer than is necessary for that purpose.

6. Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

1.4 What is Personal Data?

The GDPR defines personal data as any information that can identify a living individual either directly or indirectly, this could be name, but also includes hospital numbers, NHS Numbers and employee numbers as the identification numbers if entered onto a system can lead to a person being identified.

GDPR extends the definition of personal data to biometric and genetic data such as fingerprint and retinal scanners. Internet Protocol (IP) addresses is unique to an individual's browsing history therefore also falls under the scope of GDPR

To process Personal Data, organisations must have a lawful basis, as defined in Article 6 of GDPR

1.5 What is Special Category Data?

GDPR defines any personal data relating to race, beliefs, health or sexual life of a living individual as Special Category Data. If an organisation wishes to use special category data, it must have a lawful basis under Article 6 and also Article 9 of the GDPR.

SECTION 2 – DUTIES AND RESPONSIBILITIES

All staff working on behalf of the East Suffolk and North Essex NHS Foundation Trust are responsible for adhering to the GDPR and for maintaining patient and staff confidentiality.

An Information Governance clause is incorporated into the Principle Statement of Conditions of Employment for all staff. A breach of confidentiality, whether directly or indirectly, is a disciplinary offence that could result in dismissal and/or prosecution under the GDPR.

It is a legal responsibility of organisations to ensure that transfers of personal information for which they are responsible are secure at all stages.

SPECIFIC RESPONSIBILITIES

- The Information Governance Lead is the Data Protection Officer and responsible for this policy and leads the Data Protection agenda at the Trust on behalf of the Caldicott Guardian.

- The Caldicott Guardian is the Trust Medical Director and is responsible for confidentiality at the Trust at Board level.

- The Senior Information Risk Owner is the Director of ICT and is responsible for information security risks

- The Information & Records Governance Group is responsible for ensuring that the Trust has the appropriate policies in place and monitors compliance with Data Protection.

- The Director of Governance is the accountable director for information governance

- Line managers are responsible for disseminating this policy to their staff and ensuring that all their staff attend induction and complete annual mandatory Information Governance training.

Following the national Caldicott Committee's Report on the Review of Patient-Identifiable Information published in December 1997, every NHS Trust has a duty to appoint a Caldicott Guardian.

The Caldicott principles are concerned with the use and protection of patient-identifiable information. All Trusts must abide by the principles for all patient-identifiable information flows:

Principle 1 – Justify the purpose(s) for using confidential information.
Principle 2 – Only use it when absolutely necessary.
Principle 3 – Use the minimum personal data required.
Principle 4 – Access should be on a strict need-to-know basis.
Principle 5 – Everyone must understand his or her 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.

SECTION 3 – DATA PROTECTION PROCEDURES

3.1 Overview

The Trust's compliance with the General Data Protection Regulations (GDPR) ensures that it treats personal data in a confidential manner. A principle aim of the GDPR is to promote openness in the processing of personal data and therefore the Trust must ensure that Data Subjects know the reason their information is collected, its uses within the organisation and to whom, and the circumstances when, it may be disclosed.

The GDPR can only be applied to records relating to living individuals. However, a duty of confidence is still owed to the deceased and their families so this policy includes information on the Access to Health Records Act 1990 and the Common Law Duty of Confidence to provide guidance on this type of data.

3.2 Authorised Employees

Staff should only have access to personal data in the following circumstances:

- Where they are involved in that person's healthcare.
- For personnel/HR issues, where the employee is authorised to access personnel files.
- Where the employee is authorised to access personal data in specific circumstances e.g.:
    - Legal services in medico-legal cases and complaints
    - Clinical auditors
    - Clinical coding
    - Medical records team
    - Investigating officers
    - Finance staff for recharging Clinical Commissioning Groups for patient treatment at the Trust

3.3 Access to Personal Data

There are procedures in place to ensure that appropriate access to care records systems is provided to those members of staff who require access as part of their role.

If staff change role, they must ensure they inform IT to remove any legacy access that is no longer required in their new role.

All clinical records should be kept secure. There should be a barrier (eg locked filing cabinets, passwords on computer systems, locked office doors) between clinical records and unauthorised access.

All departments holding confidential files should have a locked filing cabinet for these records and access to the filing cabinet should be limited to authorised personnel.

Staff must **never** access their own medical record or information treated in confidence – copies of records need to be applied for from the Access to Health Records Team, or HR for Personnel files Staff must also **not** access records of people they know (whether a relative or not) without a legitimate clinical reason for doing so.

3.3.1 Access to Staff Data

Personal data relating to staff is also protected in confidence therefore subject to the same GDPR legislation. Staff that wish to request their own personnel file are to contact the IG Team directly

3.3.2 The Telecommunications (Lawful Business) (Interception of Communications) Regulations 2000

Under these Regulations employers are permitted to intercept communications of its employees, without their consent, for strictly defined purposes including preventing or detecting a crime, investigating alleged unauthorised use of the email system or to protect a life.

If the Trust receives a request to intercept an employee's work email account without their knowledge or consent, approval must be sought prior by the following staff:

- Data Protection Officer
- Data Security Manager
- Senior member of HR team

The interception can only be undertaken by a senior member of the IT team once this approval has been sought.

3.4 Telephone

- Do not make telephone calls relating to sensitive or person identifiable information where you can be overheard.
- Turn the message volume down on your answer phone so that messages cannot be overheard by unauthorised people.
- The hospital sometimes receives calls from 'bogus callers' who attempt to glean information to which they are not entitled. When you receive a telephone call, check to ensure that you are speaking to the correct person, by verifying date of birth or GP or calling back a number that you can verify independently. If the caller claims to work for an organisation and they are not known to you, ask them for their Switchboard number and offer to call them back. If you suspect a caller is bogus, do not release the information and report the incident onto Datix the incident reporting system.
- Recorded telephone messages containing person identifiable or sensitive information should only be accessible to those who are entitled to listen to them. A deputy should be appointed for times of absence and messages dealt with promptly and removed from the answering machine.
- If you need to leave a message on an individual's voicemail i.e. a patient, do not divulge any appointment details unless you are certain the messages cannot be picked up by any other individuals i.e. a spouse

- Do record a personalised message on your answer phone so that people can be sure they have dialled the right number before leaving a message.

3.5 Fax/e-Fax

In line with the NHS Standard Contract 2015/16, all discharge summaries are to be sent by electronic secure means. It is not permitted to send this information by fax
Faxing of patient information should be avoided where possible and only used when absolutely essential

If faxing is absolutely necessary, please follow the below guidance:

- Only send to a safe haven fax
- Use the minimum amount of data to identify the patient/member of staff eg patient initials and hospital number or NHS number.
- Always use a fax header sheet and mark the fax 'Confidential'.
- Indicate on the header sheet the total number of pages that the fax contains.
- Ensure that the number you are dialling is correct - check it with the recipient.
- Confirm with the recipient that the fax has been received.
- When receiving a request for person identifiable or sensitive information by fax, check that the source is genuine.

3.6 Email

Where email is used to send sensitive information, this should be clearly indicated in the subject header, for example marked 'Confidential'. No service user identifiable information should be contained in the subject heading.

If communicating with a patient via email, always gain consent. An email consent form is available on the intranet and should be uploaded onto Evolve when complete.

Follow these rules:

- Don't send bad news via e-mail.
- Keep information to an absolute minimum.
- Use only the email address that is on the consent form or an email communication from the patient.
- When you are away from your desk please use your out of office message with alternative contact details.
- Do not communicate with a third party unless it is the representative of a child and they have signed the consent form.
- Please always check the email address as part of the standard demographic checks when a patient attends hospital.
- Do not send copies of letters to patients from Evolve. These types of requests still need to be handled by the Access to Health Records Team

Consent to use email

- Complete a consent form with the patient or their representative.
- If verbal consent is given over the phone, please note this on the form.
- If a patient sends a communication by e-mail, this is deemed as implied consent.
- The form must then be filed in the patient notes or sent to the scanning department.
- A supply of forms will be available at all reception areas and ward areas.
- Keep copies of e-mail correspondence – to be filed in notes or scanned / uploaded.

Emails containing person identifiable information must be stored appropriately on receipt eg incorporated within the health record, or saved into a folder on a shared network drive, and deleted from the email system when no longer needed.

Any bulk transfers of unencrypted data must be essential for patient care, and specifically authorised by the hospital's Caldicott Guardian (the Medical Director).

- Be careful about forwarding emails which might already contain personal identifiable or sensitive details that may no longer need to be included.
- Regularly review any hospital staff where you have given them permission to access your email on your behalf, and remove their permission if necessary.

Sending an Encrypted Message

You can send an encrypted message from your nhs.net account to any email account. The recipient has to sign up to the encryption service. Please note the encryption feature will only work if you send from an nhs.net email address. Detailed guidance on how to send an encrypted message is available from IT.

Internal email

If you need to send an internal confidential email containing personal data, it must be encrypted.

This includes internal emails relating to confidential staff issues.

If staff are simply emailing a patient hospital number and initials, this is classed as pseudonymised data and does not require encryption. The patient's NHS number is classed as personal data as can be used in any Spine enabled system therefore if contained in an email, internal or otherwise, must be encrypted.

NHS Colleagues are advised to set up individual nhs.net accounts to send encrypted emails. Please contact the Service Desk to set up an account

If you need to send regular internal emails containing person identifiable or sensitive information to other hospital staff, ask the Service Desk to set you up a shared folder on the Communications drive and tell them whom you want to have access.

External email

If you send from an NHS mail account (nhs.net) to any of the following email addresses they will be secure:

- nhs.net
- gov.uk
- gov.uk
- cjsm.net
- mod.uk
- parliament.uk

Some nhs.uk have been accredited to the Secure Email Standard but very few have. If in doubt, please check with the IG Team first.

3.7 Social Networking

Many of us use the Internet at home for personal use including participating in social networking websites such as Facebook, My Space, You Tube or use Twitter or Blog websites.

You must consider the potential impact on confidentiality, your own reputation, that of the Trust and the NHS in general. You are expected to behave responsibly, professionally and in accordance with your professional codes of conduct and the Trust's values and policies.

You should not:

- Make personal (e.g. derogatory, defamatory or offensive) comments about patients, colleagues, your role or about the Trust or NHS
- Be pictured in activities, or make comments that may be open to misinterpretation
- Give out any information relating to patients, colleagues or visitors or any other personal identifiable data
- Use your Trust @esneft.nhs.uk email address or @NHS.net account on any of these sites
- Engage in activities that could bring the Trust or your profession into disrepute
- Provide new or updated information relating to yourself as a Trust employee or other staff or any services relating to the Trust on non NHS websites without first obtaining written approval from your line manager

Use of Photographs or Videos on Social Media

You must not post photographs or videos of yourself or your colleagues taken at work in the Trust, nor of patients or visitors within the Trust, nor of Trust holdings or logos. The only exceptions to this are by the written agreement of the Head of Communications, for example in health education campaigns.

3.8 Post

If the internal mail system is being used to receive person identifiable or sensitive information, it is essential that physical security measures, such as key coded or swipe card entry, are in place to protect information in the post-room, post collection point or similar.

Post

The chosen transfer method should be secure and cost effective.

- Ensure that if correspondence contains any person-identifiable information, it is marked 'Private & Confidential' and is in a sealed envelope.
- Ensure that post is sent to a named person.
- Patient identifiable information that is extensive (eg a set of copy records) or relates to more than one person should be sent by Tracked Delivery.
- Special Delivery should be used for extremely sensitive information or batches of information.

3.9 Photography

Staff

Photography or filming by staff is not permitted in any public areas throughout the Trust unless consent is sought from the Head of Communications

Staff must never use their personal smartphone to film or to take clinical photographs. For clinical photography, please refer to the Clinical Photography Policy.

Patients/Family/Visitors

Communication between patients and family is an essential part of providing support to a patient who is admitted to the hospital. However, patients must also respect the privacy of other patients and staff. Nurses in Charge are to agree the use of mobile photography or filming by patients or visitors in a clinical area. Please see guidance from the Information Governance Alliance for more information.

Patients have the right to make an audio/visual recording of their consultation with a healthcare professional as it is deemed as a form of 'note taking'. Consent from participating staff members should be sought. Any recordings generated by the patient are not the responsibility of the Trust and therefore is not liable for safeguarding the confidentiality or security of such material. Please see guidance from NHS Protect for more information.

3.10 Safe Haven

The term 'safe haven' means a location where arrangements and procedures are in place to ensure person identifiable or sensitive information can be held, received and communicated securely.

Safe haven procedures should be in place in any location where large amounts of person identifiable information are being routinely received, held or communicated. Such information should be sent from and received to a secure and protected point. All points of receipt should be considered i.e. transcribing of phone messages, fax in-trays, electronic mailboxes, pigeon holes and in-trays for paper information etc.

In non-clinical areas, each site or department should have at least one designated safe haven contact point.

General requirements for a safe haven - location/security arrangements

- A room that is locked or accessible via a coded key pad.
- If a safe haven is sited on the ground floor, any windows should have locks on them. If this is not possible, all computers should be encrypted, laptops should be secured to desks with Kensington locks, and personal and sensitive information kept locked in cabinets.
- Manual paper records containing person identifiable should be stored in locked cabinets. All departments holding personnel files should have a locked filing cabinet for these records.
- Computers and screens should not be accessible by unauthorised staff and computer users should either lock the screen or log out of the computer when it is not in use.
- Equipment such as fax and answering machines in the safe haven should ideally have an access code password.
- Answering machines should be left on low volume to avoid messages being overheard by unauthorised people.

3.11 Confidential Waste

- Ensure that all confidential waste is disposed of in the confidential waste sacks or designated lockable bins
- Ensure that confidential waste sacks are kept secure when in use. When awaiting collection bins should be kept in a secure place.
- A certificate of destruction from the specialist contractor is required for each collection of waste destroyed, which is to be delivered to the Information Governance Manager.

- Staff are not to open the bins once sealed unless in an emergency situation and with authorisation from the Information Governance Manager.
- Electronic or telephony equipment that is no longer required may contain personal data. Therefore must be sent to the Technical Support Team, IM&T for secure destruction.

3.12 Computers

- Never share your Smartcard or leave it logged in and unattended.
- Ensure that screens are sited so that unauthorised people cannot read information displayed on them.
- Electronic records containing person identifiable or sensitive information must be stored appropriately (**not** on your computer's desktop, or personal C:\ or H:\ drive).
- Lock your computer screen if you leave it unattended.
- Do not share your password with anyone and keep passwords secure.
- Never tick the 'remember me' or 'remember my password' box when logging in.
- Do not enter person identifiable or sensitive information onto web sites unless you are sure that it is the genuine web site and that there is a secure link.
- Ensure any incoming removable media is virus checked before use and report any suspected viruses immediately to the IT Service Desk.
- Never save hospital work to your personal home computer.
- Keep equipment such as laptops secure when they are not on the hospital site. Do not leave them in your car overnight
- Never dispose of computer or telephony equipment yourself. Always contact the Service Desk to arrange secure collection

3.13 USB Sticks

- Only encrypted hospital-issue memory (USB) sticks must be used to store or transfer confidential information. These are available from the Service Desk.
- Do not hand write the password on a USB stick

3.14 Mobile Devices

- Staff must not store person identifiable data on mobile devices unless they are Trust issued or rebuilt/ configured to meet Trust security standards
- Mobile devices must be pin protected
- Mobile applications containing PID must be password protected

3.15 SMS Text Messages

Key considerations when using text messages are:

- Is the mobile phone number correct?
- Is the mobile phone receiving the text message being used by the intended recipient of the message?
- Has the message been received, and what provision is there to audit message receipt?
- Text messages are normally stored on SIM cards and are typically only cleared when overwritten - as mobile phones are easy to misplace or may get stolen, there is a danger of a breach of confidentiality occurring that the patient / service user may find distressing or damaging.
- Text messages should not be used to convey sensitive information and the use of text messages for the transfer of personal data should be kept to a minimum.

- When consent is sought for appointment reminder services, service users should be informed of what information will be included in standard SMS messages sent to them via the service and the option to opt out must be available on request.

3.16 Printers and Photocopying

- Use a confidential waste sack/bin for spoiled prints and copying.
- Check that you have collected all your printing/copying and originals from the machine.

3.17 Sharing Information

Sharing information with other health care organisations

It cannot be assumed that identifiable health information can be automatically shared with any other health professional or health service employee. Care must be taken to ensure that disclosures are not made inadvertently, that those receiving the information in a professional capacity also have obligations to maintain confidentiality, that only information necessary to achieve the objective is disclosed, and it is understood that the information should only be used for the purpose for which it is disclosed.

Sharing information with non-NHS organisations

Employees of the hospital authorised to disclose information routinely to other organisations outside the NHS must seek assurance that we have a Data Sharing Agreement in place. Information must be sent to other organisations in accordance with this policy and procedures.

3.18 Loss of Data

Any loss or breach of personal data held in confidence must be reported to the Information Governance Team and also reported via Datix (the incident reporting system) immediately. Under GDPR, breaches that are classed as Serious Incidents Requiring Investigation (SIRIs) must be treated in accordance with the SIRI process and reported to the Information Commissioner's Office within 72 hours once the organisation has become aware of it.

3.19 Transfers of Personal Data outside the UK and EEA

The Information Governance Team must be consulted prior to personal data being transferred outside the UK to ensure there are appropriate safeguards in place

3.20 Offences under the DPA

The Information Commissioner's Office (ICO) has the power to order organisations to pay up to €20 million, or 4% of annual turnover, as a penalty for serious breaches of the GDPR. Under Section 170 of the Data Protection Act 2018 the ICO can prosecute individuals that knowingly or recklessly obtains personal data without the permission of the data controller

3.21 Data Subject Rights

Individuals have certain rights under the GDPR including:

- Right of Access
- Right to be Informed
- Right to Rectification
- Right to Object
- Right to Restrict Processing

- Right to Withdraw Consent
- Right to Data Portability
- Right to Data Erasure
- Right to Complain

These rights are not absolute and will be each be dealt with on a case by case basis. Approval where necessary will be sought from the Caldicott Guardian

Right of Access

All data subjects, or in certain circumstances someone acting on their behalf, can request a copy of their personal data held by the Trust. All applications regarding patient personal data must be made in writing to the Access to Health Records Team.

Employees or former employees who wish to have copies of their Personnel files must make a request in writing to the Information Governance team at FOI@esneft.nhs.uk

Staff are reminded that work emails or any written/audio-visual documents are the property of the Trust and therefore are covered under the remit of a subject access request and may be released to individuals in certain circumstances
A number of CCTV cameras are present in the Trust as part of its commitment to protect staff, patients and visitors to the Trust. CCTV is covered under GDPR and the same Subject Access Request guidance applies.

Requests for copies of CCTV are to be made to the Head of Estate Compliance and Risk Management

Please refer to the Subject Access Request Policy for specific procedures and process

Details of how individuals can exercise their other rights are published on the Trust's Privacy Notice on the Hospital Website

3.22 NHS Counter Fraud Authority

This is concerned with dealing with requests for information from the NHS Counter Fraud Authority or Local Counter Fraud Specialist (LCFS) in the prevention, detection and investigation of potential or actual crime. The Trust must co-operate with the CFSMS under these circumstances and can do so without the data subject's consent.

3.23 Police

All requests from the police for personal data will be dealt with on a case-by-case basis via the IG Manager, Caldicott Guardian, (or other Director on call), who will decide if the information can be disclosed. To release information to the Police, or another enforcement agency, without the data subject's consent, the following grounds must be met:

- There must be an overriding public interest such as to safeguard an individual's safety,
- Another lawful basis to release information i.e. under the Road Traffic Act
- A court order

The most likely legal basis for disclosure (without the patient's consent) to the police are:

- Prevention of Terrorism Act (1989) & Terrorism Act (2000)
- The Road Traffic Act (1988)

- Court Order
- HM Government (2015) Prevent Strategy

3.24 Disclosing Locations of Patients who have been admitted

Callers and/or visitors could ask at any time and at any Trust department for details about a patient's admission and which ward the patient is staying on. Staff should check on admitting a patient whether they wish callers/ visitors to have this information. If a patient does not wish callers to have this information, the appropriate Ward Reception or South Reception should be informed.

3.25 Data Protection Compliance and Confidentiality Audits

In accordance with Article 34 of the GDPR, Data Protection Impact Assessments (DPIA) must be completed when a new project/system incorporating the processing of special category data on a large scale is planned to be implemented. The DPIA is to be completed prior to implementation/commencement and approved by the Information & Records Governance Group.

It is the responsibility of the Data Protection Officer to provide advice and recommendations in relation to DPIAs. Any risks associated with the processing of large scale special category data that cannot be mitigated, are to be referred to the Information Commissioner's Office to approve processing of the data

The Information Governance Team will periodically carry out data protection and confidentiality compliance checks on existing processes and a report will be made to the appropriate department manager and the IRGG Group.

Staff are reminded that computer systems can audit their access and requests to audit an individual staff member's activity can be undertaken at any time

Such requests must be authorised by the Information Governance Manager or Caldicott Guardian

3.26 Security and Confidentiality Breaches

All security and confidentiality breaches must be reported by completing a Datix incident reporting form and notification to the Information Governance Team and appropriate line manager.

All breaches of confidentiality will be investigated. The Information Governance Team will provide investigating officers with advice on suspected breaches of confidentiality. The Data & Security Administrator, the Information Governance Manager, and the Trust Security Manager may share details of confidentiality breaches to ensure appropriate action is taken.

In accordance with the Trust's Disciplinary & Procedures Policy, action will be taken against members of staff who are negligent or commit a deliberate breach of the DP Act.

Where an information governance breach meets externally reportable criteria as set out in the NHS Digital 'Notification of Data Security and Protection Incidents' guidance, the Data Protection Officer or a designated deputy will report these onto the Data Security & Protection Toolkit within 72 hours of the organisation becoming aware of it. Reporting onto the Data Security & Protection Toolkit automatically notifies the Information Commissioner's Office.

3.27 General Security

- Paper must not be re-used for any purpose – all printed/written paper must be disposed of in the confidential waste.

- Do not allow unauthorised people into areas where confidential information is held unless they are supervised.
- Do not hold keypad lock/swipe card protected doors open for people following you in.
- Do not wedge open security doors and check that windows are closed/locked at the end of the day.
- Do not share door security codes with unauthorised people.
- Operate a clear desk policy. Do not leave confidential information out overnight.
- Wear your Hospital identity badge so that other members of staff know who you are.
- Person identifiable information should be kept in locked rooms/drawers/filing cabinets.
- Take measures to prevent casual observation of person-identifiable or sensitive information e.g. remove case notes from unmanned reception areas. All person identifiable and/or sensitive records must be stored face down in public areas and not left unsupervised at any time.
- If a patient needs to attend more than one department within the hospital and his/her hospital information is required, then the patient data must be placed in a sealed envelope and an explanation should be given to the patient that it must only be opened by the receiving clinician.
- Ensure confidential conversations are held in an appropriate place.
- Gain patient consent before sharing personal information with relatives or friends.
- Store nursing notes in wards securely, away from patient areas. Minimal nursing notes can be stored in patient bays**. Visitors are not allowed to access a patient's notes** unless through the Access to Health Records Team
- Any medical notes should be checked by clinicians before patients see them, to check for any information that might cause the patient harm or distress to read.
- Forward any requests from patients for copies of their notes to the Access to Health Records team.
- Personal data or any other confidential data stored in a paper format is not to be taken off-site unless you are authorised to do so
- When taking Trust equipment and belongings off site, store them in the boot of the car and where possible do not leave them in your vehicle overnight
- If staff are taking paperwork off site to visit community patients, use a lockable storage box/bag to store the paperwork whilst in the community
- Handover documentation for staff should only contain the minimum data required and must not be taken off a ward/clinic and disposed into confidential waste when no longer required

3.28 Key Related Documents

- Information Governance Group Terms of Reference
- Freedom of Information Policy
- Information Governance Strategy & Plan
- IM&T Security Policy
- Data Encryption Policy
- Removable Media Policy
- Disciplinary Policy & Procedures
- Subject Access Request Policy & Procedures
- Personal Electronic Devices Acceptable Use Policy

3.29 Cyber Security

All staff (including bank and contractors) must remain vigilant when processing personal identifiable data electronically i.e. submitting online forms or emailing. If staff receive an email from someone asking for confidential details or requesting payment and it is not expected or the sender is unknown to you, staff should follow the guidance below

- Do not click on links or open attachments
- Always question if you receive a request for payment outside the proper channels
- Do not use your NHS email address to subscribe to mailing lists unless work related
- Delete suspicious emails – do not reply
- Report suspicious activity to the Service Desk

3.30 Instant Messaging Applications

Staff are permitted to use WhatsApp or equivalent in connection with their role, however they must follow Trust guidance on its usage.

WhatsApp must **never** be used in the following circumstances

- To communicate confidential person identifiable data
- To communicate directly with patients or their family members/parental guardians
- To send clinical photographs
- To discuss any clinical practice/advice regarding a patient i.e. increase the patient's dosage by x amount

Staff are reminded to refer to the Social Media Policy and must always remember to respect each other's confidentialty

3.31 NHS Chaplaincy and Non-Religious Pastoral Support

Chaplains are employed by the NHS and other healthcare organisations for their expertise in providing *spiritual, pastoral and religious care*. Chaplains come from many different religions and beliefs but are united by their compassionate concern to support those who are challenged by illness and injury.

There are no IG considerations that prevent Chaplains from being visible on their healthcare premises and striking up informal conversations with patients and families

Chaplain employees can access health data within a patient's record if the patient has given explicit consent. For example they have been asked by a member staff if they would like to see a chaplain. Or the patient has previously consented to a Chaplain visit and have asked him/her to visit again, if they are readmitted to the hospital.

This must be clearly documented in the patient's record and consent can be withdrawn at any time.

Chaplains must only access records to document their visits and review previous chaplaincy notes. Access to the other sections of the patient record must be restricted

Detailed guidance is available from NHS England

3.32 NHS National Data Opt Out

This national policy enables patients to opt out from the use of their data for research or planning purposes, in line with the recommendations of the National Data Guardian in her Review of Data Security, Consent and Opt-Outs.

Patients log their choice centrally with NHS Digital and the Trust implements processes at an organistional level to ensure patient's choices are complied with

By 2020 all health and care organizations are required to be compliant

SECTION 4 – TRAINING AND EDUCATION

The Trust provides data protection and cyber security training as part of the mandatory training programme to all staff irrespective of their experience or grade.

It is a mandatory requirement for all Trust employees to complete Information Governance training at induction and complete a refresher session and successfully pass an assessment once per year.

Training is available online via Moodle

Information Governance training compliance must be above 95% for all areas.

SECTION 5 – DEVELOPMENT AND IMPLEMENTATION INCLUDING DISSEMINATION

The Information Governance Lead is the author of this document, which was reviewed by the Information Governance & Records Group.

Hospital staff will be notified of the existence of this document by means of dissemination via the IRG Group. Line Managers are responsible for ensuring their staff are aware of the contents of the latest version, which will be uploaded to the hospital's intranet.

SECTION 6 – MONITORING COMPLIANCE AND EFFECTIVENESS

The Information Governance Team will undertake the following audits quarterly:

- Completing IG spot checks, also known as GDPR MOTs in all areas to check who is using the patient administration system, which patients staff are looking at, PC screens are locked when not in use, Smartcards are not left in computers unattended etc.

- Completing data protection compliance and confidentiality checks for existing processes, software and hardware.

- Reviewing entries on Datix on a monthly basis and reporting incidents to the Information & Records Governance Group at its quarterly meetings.

SECTION 7 – CONTROL OF DOCUMENTS INCLUDING ARCHIVING ARRANGEMENTS

The Information Governance Team will review this policy regularly to ensure that it is up-to-date with current legislation and best practice guidelines.

7.1 Once ratified by the Information Records and Governance Group, the Responsible Officer will forward this document to the Information Governance Department for a document index registration number to be assigned and for the document to be recorded onto the central hospital master index and central document library of current documentation.

7.2 In order that this document adheres to the Hospital's Records Management Policy, the Information Governance Department will:

- Ensure that the most up-to-date version of this document is stored on the documentation library.
- Archive previous versions of this document.

- Retain previous versions of this guideline for a period of time in accordance with the NHS Records Retention and Disposal Schedule.

SECTION 8 - SUPPORTING COMPLIANCE AND REFERENCES

This document will support the hospital's compliance with:

- Caldicott Report (1997) (2013) (2017)
- Data Protection Act 2018
- General Data Protection Regulation
- NHS Confidentiality Code of Practice 2003
- Health & Social Care Act: Section 60
- Freedom of Information Act 2000
- Access to Health Records Act 1990
- Human Rights Act 1998
- Common Law Duty of Confidence
- Information Governance Alliance
- NHS Protect
- Information Governance: Chaplaincy and Non-Religious Pastoral Support (NHS England)