echogenicity

September 2019

www.echogenicity.co.uk

Personal Identifiable Data Security Policy 2019

Scanning Cornwall's Hearts

Table of Contents

Next Review 2021

1. Introduction

A key Information Governance requirement for all NHS organisations is to implement appropriate safe haven policies, procedures and practices to protect the confidentiality and integrity of Person-identifiable (PID) and sensitive data. The term 'safe haven' refers to a location situated on NHS premises or upon the premises of a non-NHS organisation that is required to receive, process, store or handle in any way PID and sensitive data. In order to successfully implement an appropriate 'safe haven', appropriate physical, electronic and procedural controls need to be defined and implemented in full.

Whilst Information is constantly being transferred between people, departments and organisations, it is vital that PID and sensitive information is transferred with appropriate regard to its security and confidentiality. Mapping such data and information flows and keeping an up-to-date information asset register will support Echogenicity in identifying how personal identifiable information is transferred into and out of the organisation. It will also provide the basis for NHS Echogenicity and the hosted organisations to assess the overall risks – particularly confidentiality risks - and ensures that there are sufficient physical, electronic and procedural controls in place to mitigate these risks.

PID data relates to information about a person which would enable that person's identity to be established by one means or another. This could be as explicit as a person's full name and address or it can be more subtle but equally identifying including for example an unusual surname or isolated postcode or items of different information which if taken together could allow the person to be identified. When determining whether information is PID, all information that relates to an attribute of an individual should be considered as potentially capable of identifying them to a greater or lesser extent. An outline of PID would include:

- personal details of any patient such as their name, address, postcode, telephone number, etc; and
- any information relating to diagnosis, prognosis or treatment of patients where this is linked to details that may enable the person to be personally identified.

When handling PID, it is also a requirement to comply with the Caldicott Principles:

- Justify the purpose for using confidential information;
- Only use it when absolutely necessary;
- Use the minimum that is required;
- Access should be on a strict need to know basis;
- Everyone must understand their responsibilities; and
- Understand and comply with the law.

However, there can be occasions when there is confusion over whether data may be classed as PID. If there is any doubt, the information should be considered 'PID' and further clarification sought from the Risk Manager.

In addition to PID, there are requirements to handle sensitive information. Sensitive information can be broadly defined as that which if lost, misdirected or compromised could affect individuals, organisations or the wider community. This is wider than, but includes data defined as 'sensitive' under the Data Protection Act 1998 which of course includes health information.

Finally, this Policy applies to the handling of data and information for live patients and deaths.

2. Policies statement

The Policy is intended to achieve the following Information Governance Objectives:

Confidentiality – Access to PID and sensitive and information must be confined to only those users with a specific authority to view the data (i.e. only an employee with a legitimate business/clinical need to view or access information will be permitted to do so);

Integrity – PID and sensitive data must be complete and accurate and there must not be any unauthorised alteration or deletion;

Availability – PID data and information must be available and delivered to the right person, at the right time when it is needed (i.e. this information will be made available in a secure and appropriate manner); and Accountability – Users must be held responsible for their access to and use of PID.

Accountability must be implemented by ensuring that only valid users are able to access PID and sensitive data. In addition, accounting and audit mechanisms, where available, will be employed to log access to all relevant devices and data.

3. Scope of this policy

This Policy is applicable to all members of Echogenicity (including local presences) and hosted organisations staff that regularly handle more than 100 patient records or patient records extracts containing PID and/or sensitive data.

This Policy applies to Echogenicity and hosted organisations information, information systems, networks, application systems and users including any systems managed by third-parties. This Policy applies to all sites used by the organisation and applies to all those having access to information, either on site or remotely. This includes, but is not limited to: staff employed by the organisation; those engaged in duties for the organisation under a letter of authority, honorary contract or work experience programme; volunteers and any other third party such as contractors, students or visitors.

This Policy is applicable to all electronic data held on servers, PCs, laptops, portable devices and/or media in transit. For the avoidance of doubt, the type of data to which this Policy applies is PID and/or sensitive data and/or record extract data – any data that can be used or can potentially be used to identify a patient in any way. This may include anonymised and pseudonymised data that, although it may not identify an individual, can be used in conjunction with other data and/or systems to identify a patient (i.e. Census Data).

Any handling of anonymised and/or pseudonymised data and/or record extract data should include a risk assessment to determine whether it is still possible to identify the identity of persons (for example by deduction via the use of 'small numbers') and where necessary further advice should be sought from the Risk Manager.

4. Who this policy applies to

Information Asset Owners

The information Asset Owner will be responsible for ensuring that this Policy is implemented in full.

Staff (including temporary staff)

All staff employed by the Echogenicity have a responsibility to ensure that:

- They work to the most up to date and relevant corporate and local Information Security policies; and
- They work to the most up to date and relevant Information Governance policies.

Responsibilities of Employees

All employed staff are responsible for carrying out their duties in line with the policies, to note new or amended policies and to contribute to policy making as necessary.

Managers

All staff with a supervisory role has a responsibility to ensure that:

- All staff have been shown how to access this policy on the Intranet policy library;
- Local induction of newly employed staff includes being made aware of the relevant policies and how it impacts their own roles; and
- Policies that they are responsible for are reviewed appropriately on an ongoing basis and are disseminated and implemented within services as directed.

5. Definitions used in this policy

Asset

Any information system, computer or programme owned by the organisation.

Authorisation

The granting or denying of access rights to network resources, programmes or processes.

Caldicott

A set of standards developed in the NHS for the collection, use and confidentiality of patient- related information.

Information Governance Toolkit

A series of Information Governance requirements, produced jointly by the Department of Health and NHS Connecting for Health.

Intranet

A private network for communication and sharing of information accessible only to authorised users within an organisation.

Network

A system of interconnected computers which allows the exchange of information network connection. An individual's access to the network usually involves password checks and similar security measures.

Software

Computer programmes sometimes also called applications.

Virus

An unauthorised piece of computer code attached to a computer programme which secretly copies itself using shared discs or network connections. Viruses can destroy information or make a computer inoperable.

Person Identifiable Data (PID)

PID is data that contains sufficient information to relate the data to a specific patient.

Portable Computing Device

Any mobile device capable of carrying and/or processing data including laptop computers and mobile phones.

Portable Storage Device

A device capable of storing data that can be moved between host computers. This includes: Portable or External hard disk drives, USB "pen-drives", ZIP drives, digital cameras, MP3 players, etc.

Removeable Media

This include tapes, floppy discs, removable or external hard disc drives, optical discs (DVD and CD), solid-state memory devices including memory cards and pen drives, etc.

There might be some overlap in the definition of certain device.

Recommendations for Independent Contractors

As all staff and third-parties are expected to comply with this and other policies, there are no additional recommendations.

Initiation, development and review of the policy

This Policy meets all relevant requirements in its initiation, development and review.

5.1. High-level Information Governance Risks

This Policy outlines how PID Risk Assessments must be conducted and how often.

However, the following high-level Information Governance risks have been identified and all staff and other users including third-parties handling NHS Echogenicity's PID and sensitive data must be aware of these:

Reputational Risk – loss of any PID and/or sensitive data could have an adverse impact upon the reputation of Echogenicity. The confidence that Echogenicity currently enjoys from the NHS ENGLAND, patients and other key stakeholders could be seriously undermined;

Patient Distress – loss of PID and/or sensitive data could lead to severe stress and trauma for our patients as information on any medical conditions could be made public.

Patients could take legal action against Echogenicity further undermining public confidence.

Some four principal patient risks have been identified by the Data Sharing Review, 11 July 2008, conducted at the request of the Prime Minister:

Indignity – unnecessary exposure of facts/suspicions, for example, disclosure of a medical condition that may cause embarrassment;

Injustice – stigmatisation resulting from wrongly disclosed information, leading to loss or denial of, for example, employment, training or credit;

Inappropriate Treatment – unwarranted interventions by agencies into the lives of individuals or their families, for example with draconian action being taken by mental health or child protection workers based on misinterpreted/un-contextualised data; and Ineffective Service Delivery – because, for example, individuals do not trust agencies sufficiently to provide full and accurate information as required.

Legal & Regulatory Risk – loss of PID data could result in action being taken against Echogenicity by the Information Commissioner if it is deemed that breaches of the Data Protection Act 1998 have occurred. In addition, the Information Commissioner, as a result of changes to the Criminal Justice Act 2008, now has the power to impose fines of up-to £500,000 upon organisations and individuals who are aware of information risks but have not taken reasonable care and appropriate steps to mitigate those risks. Any legal and regulatory action against Echogenicity would be publicised and highly damaging to confidence;

The NHS Care Record Guarantee – The NHS has published a 'Guarantee' on how it handles patient data including the duties of keeping records confidential, secure and accurate. Unauthorised access or modification of any patient data would breach such 'guarantees';

Human Rights Breaches – In a Landmark Judgement, the European Court of Human Rights found that in the case of I v Finland, a patients' Right to Family Life was breached after a hospital was found not to have maintained sufficient confidentiality of 'I's medical records. Failures in maintaining the confidentiality of patient data could be interpreted by a Court of Law as a breach of a patients' Human Rights by Echogenicity;

Staff Awareness – Staff must fully understand and comply with this Policy and all other relevant policies. Staff must understand that they must use their best endeavours to ensure that there is no loss or breach of patient data and confidentiality. Staff must understand that they may be liable for any such loss, and that any breaches of this or any other policy may result in disciplinary action including dismissal. Staff must also be aware that they may be held personally liable by the Information Commissioner, and could face fines of up-to £500,000; and Third-party Awareness – any user or third-party engaged in data handling, processing or transit on behalf of Echogenicity must comply with this Policy and all other relevant policies.

Where third-parties do not comply with this Policy or any other relevant policy, Echogenicity will reserve the right to terminate all current contractual agreements with immediate effect. Third-party providers and their staff must also be aware that they may be held personally liable for any non-compliance with their statutory requirements by the Information Commissioner and could face fines of up to £500,000

6. Risk Management

6.1. Introduction

All regular flows of PID and sensitive data will be subject to regular risk assessments by Verity Williams Curnow. The methodology for performing these risk assessments in outline is:

Defining PID and Sensitive Data – Methodology: outlining the approach to be taken in determining whether data is PID or sensitive;

Identification of PID Assets: Update and maintain all relevant PID and sensitive information assets via an Information Asset Register on a monthly basis;

Mapping Data Flows: Update and maintain all relevant PID and sensitive information flows into and out of NHS to Echogenicity on a monthly basis;

Risk Identification: Use the Information Asset Register and the Information Data flows as the basis for conducting risk assessments to identify any potential vulnerabilities in the controls employed; and Risk Management & Reporting: Maintain an 'Informatics Risk Register' and provide regular reports to the Information Asset Owners and Echogenicity Verity Williams Curnow will be required to validate and sign off the Information Asset Register and Information Data Flows.

6.2. Defining PID and Sensitive Data - Methodology

When assessing whether any data or information is potentially PID, the following test will be applied:

Does the information or dataset comprise one or more pieces of data or information which can be used either by itself or in combination with public domain data or

information (such as the census) to identify one or more persons combined with information (such as health information) about a person or persons whose public disclosure is likely to cause distress?

Annex A provides further guidance on whether any data or information is PID or potentially PID.

Identification of PID Assets

Echogenicity will conduct regular reviews of all information and datasets to identify those sources that are or potentially contain PID Information or data and/or sensitive data.

Echogenicity will conduct an immediate review of all relevant PID information and datasets upon any relevant initiatives being identified.

Relevant Information Owners will assist in the identification of any new and relevant information assets that fall or may fall within the scope of this Policy.

The list of all relevant datasets identified during the review will be recorded in the Information Asset Register.

Once the review has been completed, the need for any additional or regular reviews will be assessed by the relevant Information Asset Owners and approved by Echogenicity.

Each PID information asset will be allocated, immediately, a 'Information Asset Owner' who will be responsible for ensuring the safe, lawful processing of the PID data within Echogenicity and in any exchange with any other organisations.

The Information Asset Register will record, as a minimum, the following:

Information or Dataset name;

Information or Dataset purpose;

Information Owner;

Information or Dataset location;

Number of records;

Information or Data type, i.e. PID. PID or Sensitive;

Names of organisations, including contact details, who receive copies of some or all of the data from Echogenicity;

Names of organisations, including contact details, who send some or all of the data to Echogenicity;

Types of transfer (paper, CD, electronic file transfer, etc);

Frequency of data transfer (ad-hoc, daily, weekly, monthly, etc);

Number of records transferred;

Volume of records transferred;

Acknowledgement/receipt mechanisms;

Data security mechanism employed (NO SECURITY, encrypted, safe haven procedures, etc); and

Any information security or information governance risks and any countermeasures employed.

6.3. Mapping Data Flows

Echogenicity will conduct regular reviews of all data mapping flows utilising the methodology outlined below for the ongoing maintenance of the Information Asset Register.

Echogenicity will conduct reviews of all data mapping flows utilising the methodology outlined below for identifying and recording any new initiatives or changes and the ongoing maintenance of the information data flow register.

An outline of the methodology is:

- identification of all areas generating routine flows of PID and sensitive data;
- mapping and recording of such flows;
- the undertaking of a risk assessment for each of the information or data flows;
- Recording of all relevant risks in the Risk Register; and
- the raising of any significant risks to the Information Asset Owner, Echogenicity's Chief Executive

(see below).

7. Risk Analysis

Once the Information Asset Register and the Data Flows have been updated and documented, a full risk review will be undertaken to assess any vulnerabilities and controls weaknesses that could impact the confidentiality, integrity and availability of the PID data and other sensitive information.

Where any risks are identified which are not sufficiently addressed by existing controls, immediate action should be taken to report such risks. These risks should be presented at the earliest opportunity to the Information Asset Owner, Echogenicity the Chief Executive, no

more than 7 days after their identification.

Action to mitigate any residual risks must be identified and plans developed for their subsequent mitigation within 7 days of their reporting.

All major residual risks must be defined in the Corporate Risk Register.

8. Risk Management & Reporting

Regular reports highlighting any changes to the Information Asset Registers and PID data flows and any risks identified should be provided to the Chief Executive.

Physical Controls

Introduction

It is a requirement that a physical safe haven(s) is/ are established for Echogenicity to secure receipt and processing of PID and sensitive information.

Where Echogenicity is sending data to non-NHS organisations, the receiving organisation will confirm that Echogenicity does operate an appropriate 'safe haven' facility where appropriate with sufficient physical, electronic and procedural controls.

Data exchange agreements between Echogenicity and other organisations including non-NHS organisation will include all relevant details on the physical, electronic and procedural controls in place at the relevant 'safe haven' facility.

The following policy defines the Physical Security Controls that must be complied with when handling relevant PID and sensitive data: Echogenicity Physical and End-of-Day Security Policy.

8.1. Electronic Security Controls

Introduction

In order to ensure the secure lawful processing of PID and sensitive data, the following electronic security controls will be implemented:

PC Security: defining overall PC security controls;

Encryption: detailing the exact encryption requirements for all PID data;

Access Control: outlining the controls required to ensure that PID data access is on a strict need-to-know basis and fully authorised;

PID Data Management: highlighting the general policy requirements for handling PID data;

User & Password Management: defining the electronic controls necessary to prevent unauthorised access to PID data;

Accounting & Audit: outlining the detective and non-repudiation controls that will be implemented to complement and 'bind' with the other existing electronic controls; and Electronic Safe Haven Controls: all relevant controls identified in the most recent version of the NHS CfH Information Governance Toolkit will be implemented.

PC Security

When using computers for the input, display and processing of PID data, the following policy requirements will be complied with:

Access to any PC must be password protected;

The computer must not be shared;

All laptops must be encrypted;

PCs must not be used for storing PID and sensitive data;

computer screens must not be left on view thereby providing an opportunity for other non-authorised persons to view the data;

Computers and laptops not in use must be switched – off or have a secure screen saver device employed; and

All data and information must be held on Echogenicity or hosted organisation's network servers and not stored locally on the hard drives of PCs.

Encryption

All Laptops are encrypted through Cornwall IT – They are responsible for maintaining and make sure that laptops are fit for purpose.

All Echogenicity laptops which have access to PID are encrypted. Using an NHS sanctioned encryption product.

Echogenicity will encrypt all USB pens/HD where reasonably practical.

Recipients of USB drives must be authorised to receive the storage device by Verity Williams Curnow who must approve the user to hold and transport PID and sensitive data.

The encrypted devices remain the property of Echogenicity and must be returned when a staff member leaves the organisation, no longer has a business requirement to hold or transport confidential data, or is asked to return the device to Echogenicity for whatever the reason.

Access Control

AN Access Control Matrix will be maintained By Cornwall IT.

User & Password Management

The creation and use of generic user accounts will not be permitted.

Each user account will be owned by a specific member of staff who is both permitted and authorised to use their account.

Each user account will be protected by an appropriate password, the password being a minimum of 8 characters long and requiring a combination of alphanumeric characters.

Where passwords are created to allow access for the first time, the authorising system will be configured to force users to change their passwords.

Users most not write down or store their password in any form.

Users must not share their password with any other user or person.

Users will not share their account with any other user or person.

The user authorisation system will be configured to lock and bar any access to any account following three unsuccessful logon attempts.

Where an account is locked, Cornwall IT will ensure that user access is permitted only after performing appropriate validation checks of the user's identify and authorisation checks to establish whether the user is permitted to access such systems or devices.

When handling data sets or files protected by passwords, the passwords will not be transmitted or stored together with the data set or file. Relevant passwords will be securely stored and kept confidential and access to any such passwords will be on a strict need-to-know basis.

8.2. PID Data Management

PID data shall not be created or loaded onto devices which are not purchased or owned by Echogenicity or managed by a third-party on behalf of Echogenicity.

Loading PID data onto personal portable computing and storage devices such as laptops and MP3 players to name but three examples is strictly prohibited.

All PID data copied to portable devices and media MUST be encrypted using the NHS approved encryption product where reasonably practical Staff and contractors are not permitted to introduce or use any removable media other than those provided or explicitly approved for use by Echogenicity.

Removable media shall only be used by staff and contractors who have an identified and documented agreed business requirement.

The use of removable media by sub-contractors and temporary workers must be risk assessed and be specifically authorised.

When the business purpose has been satisfied, the contents of the removable media must be removed from that media through a destruction method that makes recovery of the data impossible. A log recording the permanent removal of data will be maintained.

Prior to permanently deleting data, advice must be sought from the Chief Executive as to the techniques that must be used.

8.3. Accounting & Audit

When available on any device or system or application, accounting functionality will be enabled. Monitored and maintained by Cornwall IT.

8.4. Electronic Safe Haven Controls

The Chief Executive will ensure that any additional electronic controls identified for 'safe havens' defined and updated in the most recent version of the NHS CfH Information Governance Toolkit are identified and appropriate plans defined and submitted for their subsequent implementation.

8.5. Procedural Security Controls

8.5.1. Introduction

To supplement the physical and electronic security controls, the following procedural controls will be implemented in full:

PID Justification & Approval: outlining the policy requirements for considering the case for using PID;

Segregation of Duties: defining the need to separate duties and responsibilities amongst staff to increase the overall assurance environment;

Change Management: outlining the change management requirements for ensuring that the impact of any changes or requests are fully considered;

Data Exchange by Removable Media: defining the policy requirements for handling PID data in transit;

Data Exchange by Facsimile: specifying the safe haven requirements for using facsimile;

Data Exchange by Email: stating that NHS mail accounts must be used for sending PID data by email;

Data Exchange by Secure File Transfer: outlining the requirements for secure file transfers;

Overseas Use: prohibiting the carriage or transmission of data overseas;

Guarding Against Loss or Theft of Equipment: outlining the policy requirements that staff must comply with for loss and theft risks;

Exchanging/Sharing Data with other NHS Organisations: specifying in particular the data sharing requirements;

Exchanging/Sharing Data with Non-NHS Organisations: again specifying in particular the data sharing requirements with third-parties;

Staff Training: Defining the key IG Awareness and in-depth training requirements for Commissioning and Informatics staff;

Audit: outlining the key audit, compliance and assurance requirements; and Procedural Safe Haven Controls: any additional procedural safe haven controls identified by the most recent version of the NHS CfH Information Governance Toolkit will be identified and implemented.

8.6. PID Justification & Approval

Echogenicity's Chief Executive will approve/disaprove all secondary use of PID and sensitive data. The Chief Executive will review the request taking into consideration the Risks Assessment and Privacy Impact Assessment.

8.8. Change Management

All proposed system, procedural and staff changes will be subject to a full change management process. The Change Management process will consider, as a minimum, the following factors when deciding whether or not to authorise the proposed change:

Impact, if any, upon this Policy;

Impact, if any, upon the information security objectives;

Risk assessments for the proposed changes;

Authorisation impacts for staff changes; and

Whether there is a need to escalate any proposed changes to the Chief Executive for further consideration.

8.9. Data Exchange by Removable Media

Removable media should not be taken or sent off-site unless a prior agreement by the Chief Executive. A record will be maintained of all removable media taken or sent off-site, or brought into or received within Echogenicity.

Where removable media has been taken or sent off-site, active confirmation that the media has arrived at its destination must be obtained. Similarly, where Echogenicity receives media from an external source, acknowledgement of its receipt will be provided.

Where there is a requirement to pass PID data or commercial or other sensitive data or information to a third party, the Policy requirements are:

Data flows involving PID data must be documented and approved by the Chief Executive prior to any transport;

There MUST be an agreed Data Sharing agreement in place between the two or more parties that the requirements outlined in this Policy will be complied with;

Authority to use the courier service must be obtained from an appropriate level of management;

Only authorised secure couriers will be used. General Post Office signed or recorded delivery will not be permitted under any circumstances;

A signature sheet will be used to capture the details of the handover/takeover of the removable media;

The data file creation will be authorised recording name/role/date/time details;

The data file will be created and the following details recorded: name/role/date/time. The disk will be 'burned' to appropriate Echogenicity media and encrypted using the NHS Approved Encryption Algorithm;

The data being transferred must be encrypted using the NHS-approved encryption application;

The password required to unlock encrypted data must not be transferred with the media, but should be sent to the data recipient using an alternative means such as NHS email, or by telephone provided the recipient is known to the individual sending the data;

The packaging used to transport the media will be sufficient to protect the contents from any physical damage that is likely to arise during transit;

The identification of the courier will be checked before handover of the media;

A telephone call will be made from the despatching organisation to the intended recipient at the receiving organisation to notify them of the despatch;

The nominated staff at the destination will receive the disks and sign the signature sheet;

The recipients will then immediately inform Echogenicity that it has received the package and that the contents are present and correct;

Where Echogenicity does not receive confirmation of package delivery, it will actively seek such clarification until it is satisfied that the package has indeed been delivered safely or that it has become lost or stolen;

The recipients will then verify that it is able to access the data and that it is the correct data. This verification will occur at the earliest opportunity and no more than 3 days. The recipient will also notify Echogenicity that it has been able to access the data and that the data is correct within 7 days of receipt;

Where Echogenicity does not receive confirmation of data access, it will actively seek such confirmation until it is satisfied that the data has been accessed correctly and that no further copies are required;

Once the business requirement for the use of the data has been fulfilled, the original disks will be sent back to Echogenicity using the same secure courier service;

A telephone call will be made from the despatching organisation to the intended recipient at the receiving organisation to notify them of the despatch;

The nominated staff at the destination will receive the disks and sign the signature sheet;

Where the sender does not receive confirmation of package delivery, it will actively seek such clarification until it is satisfied that the package has indeed been delivered safely or that it has become lost or stolen;

The recipient will decrypt the data with the independently despatched 'password' and confirm to the sender that it is able to access the data, and that the correct original data is present; and finally

Any incidences of data being lost at any stage of transit, including possible loss within any buildings, must be immediately reported via Echogenicity's Incident Reporting System.

Where there is transfer of non-personal or non-sensitive data or information, Routine Courier Services or Post Office Recorded Delivery may be employed if the data is not sent by email. The requirements for Routine Courier Services are:

Authority to use the courier service or Post Office Recorded Delivery must be obtained from appropriate level of management;

The courier will be selected from an approved list;

A telephone call will be made from the despatching organisation to the intended recipient at the receiving organisation to notify them of the despatch;

The contents being despatched will be placed in an unused sealed envelope or package;

A signature sheet will be signed by the despatching and receiving organisations;

The sender will check with the Courier Service that the package has indeed be delivered;

Where any loss of data occurs, Echogenicity will conduct further enquiries commensurate with the value of the data lost or stolen; and Where a package has been lost or stolen, the user will comply with the requirements for reporting loss or theft of equipment detailed later in this Policy.

8.10. Data Exchange by Facsimile

Echogenicity does not use fax machines – we email via the NHS secure email or if this is not possible post PID.

8.11. Data Exchange by Email

Any transmission of PID and sensitive data via email must occur via NHS mail with both the sender and receiver using NHS mail.

Where exchanges of data occur by NHS mail, Users will comply with the Email Policy.

For the avoidance of doubt, the exchange of PID data via Non NHS mail email or Internet email with other organisations is not permitted. Nor is the exchange of PID data with non NHS mail users permitted unless such users are physically located at the same premises.

8.12. Exchange by Secure File Transfer

Where exchanges of data occur by Secure File Transfer Protocol, Users will ensure that all data is encrypted to the minimum NHS Encryption Standard.

8.13. Overseas Use

Staff are not permitted to transfer any PID and/or sensitive data to any overseas location.

Staff are not permitted to take any laptops or other portable devices overseas (due to the risk of loss or theft or confiscation by a 'foreign' police force or customs department) overseas.

8.14. Guarding Against Loss or Theft of Equipment

In order to comply with this Policy and all other relevant policies, Staff must ensure that they use their best endeavours to prevent the loss or theft of any laptop, portable device or other media.

8.15. Laptops

Laptops should be carried in protective anonymous bags or cases to reduce the likelihood of theft. Any laptops that store PID should be encrypted.

When users are travelling, laptops should be kept out-of-sight and should not be left unattended unless in a relatively secure location such as the boot of a car.

Laptops must not be left unattended in car boots overnight.

Laptops must not be left unattended in public places and users must be vigilant against opportunistic theft of laptops and other portable computing devices in busy public places such as airports, train stations, hotel lobbies, exhibition halls and public transport. Users must, when using public transport, guard against leaving or storing laptops in overhead racks where they may easily be forgotten.

Laptops must not be used with removable media in places where the media could become lost or stolen.

Staff must be vigilant in ensuring that when laptops are in use, there is no possibility of information on the screen being observed by unauthorised users.

8.16. Exchanging/Sharing Data with NHS Organisations

As all NHS organisations are required to comply with the IG requirements, there are no additional policy requirements for sharing data with other areas of the NHS. However, care is still required to ensure that data exchange occurs securely (See Data Encryption).

Exchanging/Sharing data with Non-NHS Organisations

Where data exchanges with Non-NHS organisations occur or are planned, the Chief Executive will undertake a formal risk assessment.

Employees of Echogenicity authorised to disclose information to other organisations outside Echogenicity must seek an assurance that these organisations have a designated safe haven point for receiving PID data.

Echogenicity must be assured that such organisations are able to comply with the Safe Haven ethos and meet certain legislative and related guidance requirements including but not limited to:

8.17. Data Protection Act 1998;

ISO 27001 based Information Security Management System;

Common Law Duty of Confidentiality; and NHS Code of Practice: Confidentiality.

Employees of NHS the CCG authorised to disclose information to other organisations outside of the organisation or NHS must seek an assurance that these organisations have a designated safe haven point for receiving and managing PID data.

8.18. Staff Training

All staff will undergo relevant Mandatory Information Governance Awareness Training as provided by the online Information Governance Training tool or the E-learning for healthcare.

In addition, all staff who handle PID and sensitive data will undergo additional in-depth Information Governance training to ensure that there is adequate understanding of this Policy.

8.19. Audit

All Commissioning Informatics Services will be subject to regular audits to establish the degree of compliance with this Policy and provide assurance that the Commissioning Informatics Service is being managed securely and lawfully.

All audit reports will be managed in line with Echogenicity's existing arrangements for Information Governance Audits.

8.20. Procedural Safe Haven Controls

Any additional procedural controls identified in the most recent version of the NHS CfH.

Information Governance Toolkit will be identified by the Chief Executive and relevant plans for their subsequent implementation will be identified and submitted for approval.

8.21. Compliance with National Standards

Echogenicity Commissioning Informatics Services will comply in full with all relevant standards that are defined by relevant external NHS organisations.

Where there is a conflict or difference between the requirements of this Policy and of the externally defined requirements, the latter will take precedence over the requirements set by this Policy unless there is clear evidence that to do so will result in Echogenicity being exposed to any risks.

Where there is a conflict of Interest between any externally defined requirements and the requirements set by this Policy, they will be communicated immediately to the Chief Executive.

8.22. Incident Reporting

The staff will be responsible for escalating the incident, if necessary, via the Incident Reporting System.

Any member of staff who does not report immediately the loss or theft of any laptop, portable device or other relevant media may be subject to disciplinary proceedings.

For the avoidance of doubt, if any staff member is unsure whether a incident is serious enough to merit

reporting via the Incident Reporting System, they must be aware that they must report the incident regardless of any doubts that may exist.

8.23. Critical Success Factors

In order to implement and achieve an effective Information Governance culture within the Commissioning Informatics Services, the following factors will be evaluated when assessing progress in the full implementation of this Policy by the Information Governance Steering Group:

8.24. Visible support and commitment from all levels of management;

Visible support and commitment from all levels of management;

An organisation wide understanding of the information security requirements, risk assessment and risk management;

Effective marketing of information security to all managers, employees and other parties to achieve awareness;

Distribution of guidance on information security policy and standards to all managers, employees and other parties;

Provision to fund information security management activities;

Providing appropriate awareness, training and education; and Establishing an effective information security incident management process.

9. Dissemination

All staff will be made aware of the existence of this policy and its location – a hard copy will be kept in Echogenicity's Head Office.

10. Implementation of this Policy

All new and existing users of Informatics Services will be required to understand and comply fully with this Policy.

This Policy is, and will continue to be, supported by a framework of additional policies, technical standards, operational procedures and guidance, to ensure that information security requirements are understood and met throughout the organisation. As stated previously, these will be updated, where necessary following additional risk and gap analysis studies.

11. Advice and Guidance

Further advice and guidance is available from the Chief Executive.