Health and Social Care

Northern Ireland Fire & Rescue Service

Information Security

1.07 Data Transfer All User Standard

Approval

Document Reference	Information Security - 1.07 Data Transfer – All User Standard
Version	0.3
Last updated	1st March 2021
Owner	
Approval by	

Contents

1. INTRODUCTION

Health and Social Care (HSC) and Northern Ireland Fire and Rescue Service (NIFRS) (herein HSC will refer to all HSC and NIFRS organisations) Information and Information Communication Technology (ICT) (herein Information Assets and Systems), is vital to the successful operation and effectiveness of HSC organisations.

Data Transfer is the process of moving HSC information from one place to another. It could be physical movement of hard copy information, e.g. sending documents via a courier service, or digitally transferring electronic information, e.g. sending a spreadsheet via email.

Risk to the security of the Information increases where HSC organisations transfer data, for example where we rely on transfer mechanisms outside of our Information Security controls to move the information, or as legal considerations become applicable, such as transferring information internationally.

2. PURPOSE

The purpose of this Standard is to provide clear guidance on transferring information. This Standard aims to reduce the risk of any data security breaches across the organisation by ensuring the confidentiality, integrity and availability of information during the transfer or sharing processes.

3. SCOPE

This Information Security Standard applies to:

- All parties who have access to, or the use of, Information Assets and Systems belonging to, or under the control of, HSC or NIFRS [1], including:
  - HSC and NIFRS employees;
  - Temporary Staff including agency and students;
  - Voluntary Health Sector organisations / Volunteers;
  - Third Party Contractors;
  - Any other party making use of HSC ICT resources;
- HSC information stored, or in use, on HSC or externally hosted systems;
- Information in transit across the HSC networks;
- Information leaving HSC networks; and
- ICT Systems belonging to or under the control of HSC.

[1] Northern Ireland Health & Social Care organisations include Health & Social Care Board (HSCB), Public Health Agency (PHA), Health & Social Care Trusts, NI Ambulance Service (NIAS), Business Services Organisation (BSO), Patient & Client Council (PCC), Regulation & Quality Improvement Authority (RQIA), NI Guardian Ad Litem Agency (NIGALA), NI Blood Transfusion Service (NIBTS), NI Social Care Council (NISCC), NI Practice and Education Council for Nursing and Midwifery (NIPEC), NI Medical and Dental Training Agency (NIMDTA), GP Practices and other Independent Contractors to HSC, and Northern Ireland Fire and Rescue Service (NIFRS).

This Standard applies throughout the entire information lifecycle from acquisition/creation through utilisation to storage and disposal.

4. STANDARD NON-COMPLIANCE / BREACH

See the Information Security Policy for details of what to do in the event of non-compliance or a breach of an Information Security Standard. For an information Security Breach or Incident, see the Information Security Incident Identification and Reporting All User Standard.

5. DATA TRANSFER

5.1. TRANSFERRING AND SHARING PERSONAL DATA

5.1.1. Based on the information classification assigned to data, and according to local Data classification Policies, all staff must ensure the following:

- All other HSC Policies and Standards are complied with.
- HSC Data Access Agreement (DAA) template should be completed where personal identifiable data is shared for a secondary purpose (e.g. not for direct care or for a reason other than the initial purpose for which the data was collected)
- Personal data and/or confidential information is only transferred to those who are authorised to receive it.
- Information is relevant and accessed/transferred on a need-to-know basis.
- The impact to HSC and any third parties is considered before disclosing information, and where personal data, potential harm to the data subject is considered.
- Information shared is sufficient for its purpose and is of the right quality to ensure that it can be understood, used for its intended purpose, and relied upon.
- Information is accurate prior to sharing, it is up to date and clearly distinguishes between fact and opinion. If information is inaccurate, incomplete or out of date then this must be escalated in line with a local Records Management Policy.
- Third party Data Transfer processes are not fully initiated until both organisations are aware and assured on the level of security and confidentiality through a Data Sharing Agreement (DSA).

5.1.2. Where a data set contains data of multiple classification levels, the requirements of the highest classification shall be used for all data in the same transmission (for example, 20% of the data is sensitive personal data, and 80% is not, 100% must be treated as sensitive personal data, or the data must be split into separate transmissions).

5.1.3. Staff must stay vigilant when receiving requests for information and look for signs of phishing or social engineering attack. If in doubt, staff must check with the requester

using a trusted (alternative) communication method, and follow correct process before sharing information, especially if there is an unusual or greater time pressure than normal to the request.

5.1.4. Organisations disclosing information containing personal data will be subject to the Data Protection Act 2018 (DPA 2018). Disclosure of personal data is an act of 'processing', so any disclosure containing personal data must comply with all of the provisions of Part 3 DPA 2018 or the General Data Protection Regulation (GDPR).

5.1.5. HSC staff must consider the following prior to sharing personal data outside of an agreed process:

- What is the sharing meant to achieve?
- What information needs to be shared and is it proportionate?
- What HSC classification is the data, do any special measures apply?
- What risk does the data sharing pose to individuals?
- Are we allowed to share the information?
- Is the data being shared with a third party, if so is a data sharing agreement in place?
- What would happen if we did not share the data?
- Who requires access to the shared personal data?
- Does this contain any special category data?
- When should it be shared?
- How should it be shared?
- Do we need to record the decision to share?
    - How can we check the sharing is achieving its objective?
    - Could the objective be achieved without sharing the data or by anonymising it?
    - Will any of the data be transferred outside of a country or group of countries as permitted by the Data Protection Act and/or relevant legislation?
    - Do we need to review the DPIA?

5.1.6. In addition to the DPA 2018 and GDPR requirements, the 'Confidentiality: NHS Code of Practice' describes the following four requirements that must be met when handling confidential patient information:

- Protect – look after the patient's information;
- Inform – ensure that patients are aware of how their information is used;
- Provide choice – allow patients to decide whether their information can be disclosed or used in particular ways; and
- Improve – always look for better ways to protect, inform, and provide choice.

5.1.7. Third party transfers requesting disclosure of personal information from HSC organisations, must be approved by the Personal Data Guardian (PDG). Once sharing has been approved, the DSA must be developed and signed by both organisations, confirming their assent to the Data Transfer process.

5.1.8. The PDG, on behalf of HSC, reserves the right to reject an individual exchange of any personal data should they not be fully satisfied with the security and

confidentiality procedures of a third party organisation, irrespective of the DSA.

5.1.9. If disclosing personal data, under the DPA 2018 and GDPR staff must ensure:

- A Data Protection Impact Assessment (DPIA) has been completed, and is up to date, for the business process;
- Personal data is disclosed for the same specific purpose for which it was originally collected;
- Disclosure is necessary and in-line with the purpose for which it was originally collected;
- Unless there is a legal basis for processing or sharing information, it should be shared with the consent of patients. For consent to be given, patients must be informed of the purposes for which the information about them may be recorded and shared.
- Reasonable steps are taken to ensure that no inaccurate, incomplete or out-of-date personal data is disclosed;
- The recipient is provided the information necessary to allow them to assess the degree of accuracy, completeness and reliability of the data. Particular care must be taken with bulk disclosures;
- That if it is subsequently discovered that the data was incorrect or the transmission was unlawful, the recipient is notified without delay; and
- Engagement with the Data Protection Officer before any potential international transfers of personal data outside of country or group of countries permitted by the Data Protection Act and/or relevant legislation.

5.1.10. A record of data sharing must be kept, identifying the content shared, how it was shared and the protection applied, when it was shared and that receipt of the transfer has been successful at the destination.

5.2. DATA PROTECTION IMPACT ASSESSMENT (DPIA)

5.2.1. Before establishing any new form of data transfer process that involves personal data, a DPIA must be conducted as a requirement under the DPA 2018/GDPR. The DPIA initially has screening questions to assess whether there is a high risk, and if so, the full DPIA must be completed.

5.2.2. Any new data flows that arise out of a new project or procurement where HSC is the data controller or receives personal or sensitive information as defined within the Information Classification scheme will need to be recorded as part of HSC's Asset Register. Refer to the Information Security 1.04 Asset Management Standard for more information.

DATA SHARING AGREEMENTS (DSA)

5.2.3. All HSC organisations must establish DSAs when transferring HSC data between the organisation and third parties. The following information must be captured:

- The details of the two parties entering into the DSA;
- A brief description of the background and context of this data sharing

agreement;

- Details about why the personal data is processed?
- Details of whose, what and how personal data is to be shared / processed, and a map of the data flow;
- The specific basis for processing by each party;
- The relationship in terms of data controller / data processor roles;
- How the parties intend to have in place appropriate technical and organisational security, retention and disposal measures;
- How security incidents or data breaches will be handled;
- Review/termination details for the DSA;
- Declaration, indemnity and governing law and jurisdiction details.

5.2.4. The DSA shall require that the third party must:

- Act only on instructions from the HSC organisation;
- Ensure that the persons authorised to process personal data are subject to an appropriate duty of confidentiality;
- Assist the HSC organisation by any appropriate means to ensure compliance with the rights of the data subject under Part 3 of the DPA, or the GDPR;
- At the end of the provision of services:
  - Either delete or return to the controller (at the choice of HSC organisations) the personal data to which the services relate; and
  - Delete copies of the personal data by a secure method set out by the HSC organisation, unless subject to a legal obligation to store the copies.
- Make available to the HSC organisation all information necessary to demonstrate compliance with this section;
- Allow for and contribute to audits, including inspections, conducted by the HSC organisation as a controller or another auditor mandated by HSC; and
- Comply with the requirements of this section when engaging sub-processors.

5.2.5. HSC organisations must review DSAs on a regular basis to address any changes in circumstances and reassess the rationale for the data sharing activities.

5.2.6. DSA can only be approved by a Personal Data Guardian for the organisation who owns the information. If there is any doubt about whether information should be stored or disclosed, staff should speak to the local Data Protection Officer or a local Information Management specialist.

6. SPECIFIC CONSIDERATIONS WHEN TRANSFERRING DATA VIA DIFFERENT METHODS

6.1. TRANSFERS OF DATA VIA EMAIL

6.1.1. Any correspondence sent or received via HSC's email system is considered a public record and will fall under the requirements of the following:

- The Freedom of Information Act 2000 (FOI) in relation to business information;
- The DPA or the GDPR in relation to personal data.

6.1.2. All staff are responsible for ensuring the confidentiality of information they send by email.

6.1.3. Personal data must not be sent by email outside the HSC network unless proper security measures, approved by the HSC ICT department, are in place, including encryption or cloud based secure transfer services.

6.1.4. Where encryption is applied, the encrypted file and password should not be sent by the same route (e.g. if the data file is sent by email then the password must not be sent by email and should instead be sent by SMS text or a phone call) and the password must satisfy requirements within the Information Security Accounts and Password Standard.

6.1.5. Personal data must not be emailed either to or from any staff member's personal email account.

6.1.6. Personal data must not be transferred to, stored or processed on any personal device.

6.1.7. The following specific safe email transmission procedures must be followed as a minimum:

- Staff must only send the minimum information required and care must be taken to ensure the correct email address is used, e.g. when using the 'reply to all' button, that information is sent to appropriate person(s);
- Staff must not include names, addresses or other identifiable information in the subject line of an email; and
- Staff must not share confidential information, i.e. special category data, as free text, for example directly in the body of an email. Staff shall share the information within a separate document (e.g. MS Word document) and send as an attachment that has been encrypted in line with the Information Security Encryption Standard (staff must comply with the process and if unsure, must seek advice from the ICT department on how to encrypt a document).

6.2. TRANSFERS OF DATA VIA FAX

6.2.1. Appropriate controls must be identified through a risk and governance process to ensure information is faxed securely.

6.2.2. Fax machines must not be used to transmit personal data or other confidential information unless in exceptional circumstances which are approved by the Head of Department or local risk owners.

6.2.3. Fax machines shall not be used to transmit highly sensitive or business sensitive information for routine matters when other communication methods will suffice.

6.2.4. Fax machines must be located in a secured area that is restricted to authorised staff only.

6.2.5. Only staff aware and trained on the risks of using fax machines should fax information.

6.2.6. Make sure it is permissible to fax the information requested in accordance with departmental procedures. If unsure, seek the permission of a manager or other individual with appropriate authority, prior to sending the information.

6.2.7. Information should be anonymised, where possible, to limit identification of the service user or patient.

6.3. PHYSICAL MEDIA TRANSFER

6.3.1. Any media containing information needs to be protected against unauthorised access, misuse or corruption during transportation (unless already publicly available). The following shall be considered to protect media when being transported:

- Packaging must be sufficient in order to protect the contents from any physical damage during transit;
- Logs shall be kept, identifying the contents of the media and the protection applied.

6.4. TRANSFERS OF DATA VIA REMOVABLE MEDIA

6.4.1. All staff must be aware of the risks associated when removable media is used for data transfer. Refer to the Information Security Removable Media Standard for more detail.

6.4.2. Staff must ensure only approved encrypted removable media adhering to an appropriate level of encryption, as defined in the Information Security Encryption Standard, are used for the transfer of personal data or business sensitive information.

6.4.3. Staff must ensure removable media that has been approved for use within the organisation is appropriately labelled in line with the requirementsof the classification of that data.

6.4.4. Staff are not permitted to save the contents of organisation-encrypted devices onto personal devices (e.g. their home computer, laptop, smartphone or tablet) or other media.

6.4.5. Staff must only use removable media to temporarily store and transfer organisation information that is required for a specific business purpose where the use of a more secure method is not available.

6.4.6. The use of removable media by all sub-contractors or temporary workers must be

risk assessed and be specifically authorised by the ICT department.

6.4.7. See Transfers of Data Via Courier Services section for sending removable media via courier.

6.5. TRANSFERS OF DATA VIA CLOUD, INTERNET SERVICES AND DATA SHARING PORTAL

6.5.1. Staff and contractors must not introduce or use any cloud service providers (e.g. Dropbox, iCloud) to transfer data other than those provided or explicitly approved for use by the organisation, for example OneDrive using HSC credentials.

6.5.2. Line managers, in collaboration with the local ICT Department, shall be responsible for the day to day management and oversight of data sharing within HSC approved cloud, internet storage and data portals.

6.5.3. Only staff and contractors who have an identified, approved and agreed business need shall use cloud services for storage and data transfers.

6.5.4. The storage or transfer of data between secure cloud providers by sub-contractors or temporary workers must be risk assessed and be specifically authorised by the local ICT department.

6.5.5. Where the HSC secure cloud storage is being used for data transfer, the data must not be made available for longer than 72 hours (3 days) and must then be removed entirely from the online service. This is to prevent data leakage from someone compromising a cloud storage account.

6.6. TRANSFERS OF DATA VIA COURIER SERVICES

6.6.1. HSC organisations must ensure only approved routine courier services, as defined by local process, are used for the transfer of non-personal or non-sensitive business information.

6.6.2. HSC organisations must ensure only approved secure courier services, as defined by local policies, are used for the transfer of personal data or business sensitive information. Packaging must be sealed, tamper-proof and tamper-evident.

6.6.3. Staff must obtain the appropriate level of authorisation prior to the use of a courier service, as defined by local policy.

6.6.4. Care must be taken to ensure that information, other than the information required for delivery, for example the recipient’s name and address, is not accessible without breaking the seal of the envelope/package, i.e. sensitive information visible through the clear window of an envelope.

6.6.5. Specific processes must be created for frequent data transfers via courier.

6.6.6. Where removable media is being sent via courier, the media must be encrypted before transport with the decryption password sent via a different method, for

example if the removable media is sent by courier then the password must not be sent by courier and should instead be sent by email, SMS text or a phone call) and the password must satisfy requirements within the Information Security Accounts and Password Standard.

6.6.7. The packaging used for transit must ensure that the contents is sufficiently protected from any physical damage likely to arise during transit, for example physical damage caused by dropping the package or water ingress.

6.6.8. Recorded/tracked services should be used to confirm delivery.

7. MONITORING

Staff must be aware that any data on the organisation's systems remains the property of HSC. HSC reserves the right to monitor and record any use of organisation information and systems to ensure they are used for legitimate purposes, and that policies and standards are being complied with.

All monitoring must be undertaken in accordance with the appropriate legislation such as Regulation of Investigatory Powers Act (2000), Human Rights Act (1998), and good practice guidance such as "Employment Practices Code Part 3: Monitoring at Work" issued by Information Commissioners Office.

8. REVIEW CYCLE

This Standard will be subject to annual review or following any significant incidents, changes to UK or EU legislation or changes to the HSC structure or functional responsibilities.

<<Add Name>>.

<<Add Role>> Date: 03/03/2020

<<Add Name>>.

<<Add Role>> Date: 03/03/2020