

V-IG P1020 Secure Data Transfer Policy

1. Document Control

1.1. Document Approval

Document Control Sheet Title:		V-IG P1020 Secure Data Transfer Policy	
Electronic File Name (if different from above):		N/A	
Consultation with:		Director of Corporate Assurance Director of Quality and Nursing	
Approval Level:		Vocare Risk Management Committee	
Dissemination Date:	TBC	Implementation Date:	tbc
Method of Dissemination:		Via Vocare Executive Directors, Regional Triumvirates and Heads of Service	
Distribution: • Essential Reading for:		All governance, operational , clinical and managerial staff	

Author(s) (name and post):	[REDACTED], Head of Clinical Governance	
Approved by:	Function	Name
	Director of Corporate Assurance/DPO	Falu Bharmal
	Urgent Care Division Managing Director	Andy Gregory
Version No:	V1.00	
Supersedes:	V-IG P 37 Guidelines for the safe transfer of patient identifiable information and V-IG P 44 Secure transfer of information	
Summary of Changes from Previous Version:	Consolidation of information from above policies. Inclusion of GDPR 2016 and DPA 2018 compliances.	
Approval Date:	23-/07/2020	
Review Date:	July 2022	
Next review date:	July 2022	

Contents

1. Document Control.....	2
1.1. Document Approval.....	2
2. Quick Reference Guide.....	4
3. Purpose	4
4. Definitions	4
5. Key Legislation and Guidance relating to secure transfers of data.....	6
6. Principles and Standards	6
6.1. GDPR Principles	6
6.2. National Data Guardian Data Security Standards	7
6.3. The Caldicott Principles	8
7. Responsibilities.....	9
8. Training	10
9. Process	10
10. Data Breaches within this Process	18
11. Involvement of External Partners	19
12. Escalation to the Data Protection Officer and to the Caldicott Guardian	19
13. Governance	19
14. Related Policies and Standard Operating Procedures	19

2. Quick Reference Guide

All staff should ensure that they understand this section fully and follow any instructions in order to minimise personal and organisational risks.

Please note: This is not a replacement for ensuring that you understand the detail of the policy document. It simply acts to remind you of the essential steps you must be taken to fulfil the needs of the organisation in relation to this

As an organisation which collects, analyses, publishes or disseminates confidential health information, Vocare has developed the appropriate structures and procedures so that all staff follow these principles regarding the secure transfer of personal or sensitive information. These systems are based on the National Data Guardian (NDG) Data Security Standards. They are applicable to patient and staff data. w

When transferring data or information staff need to take into account the nature of the information to be transferred and ensure that it has the necessary protection to ensure its security. This is especially important when information contains personal, confidential or special categories of data. This procedure sets out different types of transfer and security requirements. However, please seek the advice from the Data Protection Officer and Head of Clinical Governance if a transfer method is not included here to assess the most secure option for your transfer of data.

To ensure compliance with the principles of GDPR, routine transfers of personal confidential data and business sensitive data must be data flow mapped. This then enables Vocare to provide transparency and demonstrate integrity regarding the data flows it processes and how these are transferred securely to ensure that patients and staff trust Vocare to process their data.

3. Purpose

The purpose of this policy is to:

- Give service users and our staff confidence in the way in which Vocare processes and transfers their data.
- Inform and confirm the secure methods of data transfer allowable within Vocare, so that Vocare remains compliant with all data protection legislation and codes of practice.

4. Definitions

Personal Data - This contains details that identify individuals even from one data item or a combination of data

items. The following are demographic data items that are considered identifiable such as name, address, NHS Number, full postcode, date of birth. Under GDPR, this now includes location data and online identifiers.

Special Category Data - This is personal data consisting of information regarding: race, ethnic origin, political opinions, health, religious beliefs, trade union membership, sexual life and previous criminal convictions. Under GDPR, this now includes biometric data and genetic data.

Business Sensitive Information - This is information that if disclosed could harm or damage the reputation or image of an organisation.

Personal Confidential Data - This term came from the Caldicott review undertaken in 2013 and describes personal information about identified or identifiable individuals, which should be kept private or secret. It includes personal data and special categories of data but it is adapted to include dead as well as living people and 'confidential' includes both information 'given in confidence' and 'that which is owed a duty of confidence'.

Processing – This means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Data Security can be broken down into three areas: Confidentiality, Integrity and Availability and these are fundamental when transferring or accessing data.

Confidentiality is about privacy and ensuring information is kept confidential and only available to those with a proven need to see it. This data must not be disclosed to others unless a legal statute or patient or public interest applies. It would be unacceptable for a perfect stranger to be able to access personal confidential data from a laptop simply by lifting the lid and switching it on. That's why a laptop should be password-protected and the data on it encrypted when switched off and also when this information is transferred it must be done so following secure transfer processes.

Integrity is about information stored in, for example, a database being consistent and unmodified. Systems must be designed so that the input and management of information is not prone to human error and that the flow of information does not result in loss or alteration. Secure transfer processes such as encryption must be followed when transferring information to ensure this remains secure.

Availability is about information being there when needed. System design must include appropriate access controls and checks so that the information in the system has consistency and accuracy, can be trusted as correct and can be relied on when providing health or care.

5. Key Legislation and Guidance relating to secure transfers of data

A number of acts and guidance dictate the need for secure transfer arrangements to be set in place.

They include (but are not restricted to):

- General Data Protection Regulation (GDPR) 2016
- Data Protection Act (2018)
- National Data Guardian Data Security Standards

6. Principles and Standards

6.1. GDPR Principles

Article 5 of GDPR sets out seven key principles, these principles, in particular Art 5(f), along with the 10 Data Security Standards (detailed below) are integral to the safe and secure transfer of information.

General Data Protection Regulation 2016 (GDPR) enacted into UK law by the Data Protection Act 2018. Some areas of data processing allow the UK to have flexibility and derogations and are therefore not covered under GDPR but are covered under the Data Protection Act 2018.

The aim of the GDPR is to protect the fundamental rights and freedoms of natural persons with regard to the processing of personal data and the rules enabling the free movement of Personal Data.

All staff must adhere to the principles of the GDPR when processing personal and/or special categories of data and demonstrate compliance with these. Article 5 of GDPR sets out seven key principles which lie at the heart of this data protection regime, this includes ensuring the secure transfer of information.

Article 5 of the GDPR states that personal data must be:

- a. Processed lawfully, fairly and in a transparent manner in relation to individuals 'lawfulness, fairness and transparency';
- b. Collected for specified, explicit and legitimate purposes and not further processed in a manner that is

incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes ('purpose limitation');

- c. Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');
- d. Accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');
- e. Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals ('storage limitation');
- f. 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 ('integrity and confidentiality')."
- g. The seventh principle relates to "accountability" which makes the CCG responsible for complying with the GDPR and says that the CCG must be able to demonstrate compliance.

6.2. National Data Guardian Data Security Standards

The National Data Guardian (NDG) Data Security Standards have been developed as a result of the National Data Guardian Review of Data Security, Consent and Optouts. These outline measures to ensure information at rest and in transit is secure. There are 10 standards which are clustered under 3 leadership obligations to address people, process and technology issues. These are:

Leadership Obligation 1

People: ensure staff are equipped to handle information respectfully and safely, according to the Caldicott Principles.

- Data Security Standard 1. All staff ensure that personal confidential data is handled, stored and transmitted securely, whether in electronic or paper form. Personal confidential data is only shared for lawful and appropriate purposes.
- Data Security Standard 2. All staff understand their responsibilities under the National Data Guardian's

Data Security Standards, including their obligation to handle information responsibly and their personal accountability for deliberate or avoidable breaches.

- Data Security Standard 3. All staff complete appropriate annual data security training and pass a mandatory test, provided through the revised Information Governance Toolkit.

Leadership Obligation 2

Process: ensure the organisation proactively prevents data security breaches and responds appropriately to incidents or near misses.

- Data Security Standard 4. Personal confidential data is only accessible to staff who need it for their current role and access is removed as soon as it is no longer required. All access to personal confidential data on IT systems can be attributed to individuals.
- Data Security Standard 5. Processes are reviewed at least annually to identify and improve processes which have caused breaches or near misses, or which force staff to use workarounds which compromise data security.
- Data Security Standard 6. Cyber-attacks against services are identified and resisted and CareCERT security advice is responded to. Action is taken immediately following a data breach or a near miss, with a report made to senior management within 12 hours of detection.
- Data Security Standard 7. A continuity plan is in place to respond to threats to data security, including significant data breaches or near misses, and it is tested once a year as a minimum, with a report to senior management.

Leadership Obligation 3

Technology: ensure technology is secure and up to date.

- Data Security Standard 8. No unsupported operating systems, software or internet browsers are used within the IT estate.
- Data Security Standard 9. A strategy is in place for protecting IT systems from cyber threats which is based on a proven cyber security framework such as Cyber Essentials. This is reviewed at least annually.
- Data Security Standard 10. IT suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardian's Data Security Standards.

6.3. The Caldicott Principles

Before using or sharing confidential information, you must also consider the Caldicott Principles:

- Principle 1: Do you have a justified purpose for using this confidential information? The purpose for

using confidential information should be justified, which means making sure there is a valid reason for using it to carry out that particular purpose.

- Principle 2: Are you using it because it is absolutely necessary to do so? The use of confidential information must be absolutely necessary to carry out the stated purpose
- Principle 3: Are you using the minimum amount of information required? If it is necessary to use confidential information, it should include only the minimum that's needed to carry out the purpose.
- Principle 4: Are you allowing access to this information on a strict need-to-know basis only? Before confidential information is accessed or transferred, a quick assessment should be made to determine whether it is actually needed for the stated purpose. If the intention is to share the information, it should only be shared with those who need it to carry out their role.
- Principle 5: Do you understand your responsibility and duty to individuals with regards to keeping their information secure and confidential? Are you up to date with your training? Do you understand your responsibility for protecting information?
- Principle 6: Do you understand the law and are you complying with the law before handling the confidential information?
- Principle 7: Do you understand that the duty to share information can be as important as the duty to protect confidentiality. However, it's important to remember if you are sharing this is done lawfully and securely.

7. Responsibilities

- **Vocare's Managing Director** - has overall responsibility for the implementations of the provisions of this procedure. Acting as the Senior information risk owner, [SIRO] they are responsible for ensuring that the appropriate mechanisms are in place, with support of their co executives and directors, departmental heads, and line managers, for ensuring that all staff are aware of the secure transfer of data and information procedures .
- **Vocare's Medical Director as the Urgent Care Division's Caldicott Guardian** - has responsibility for ensuring secure transfers of data procedures are in place throughout the organisation. The National Governance Department, in conjunction with the Information Governance group, the Data Protection Officer (DPO), SIRO and the Caldicott Guardian will monitor and investigate any secure transfers of patient data breaches.
- **Totally plc's Director of Corporate Assurance as Data Protection Officer (DPO) for the Group** - is responsible for developing and maintaining comprehensive and appropriate documentation, including secure transfers of

information, that demonstrates commitment to and ownership of data security responsibilities.

- **Vocare's Head of Clinical Governance** – has responsibility for reporting relevant data breaches to NHS Digital.
- **Line Managers** - have responsibility for ensuring that all staff are aware of and understand this procedure.
- **Employees** - have a responsibility for ensuring the information is handled, used, stored and shared confidentially and appropriately. If in doubt individuals should seek guidance from their line manager in the first instance, or the National Governance Department. assurance@nduc.nhs.uk. Any issues should be reported in the first instance on Datix.

8. Training

Training is mandated as part of the annual information data security and awareness training modules.

9. Process

Physical elements

- Secure Transfer of Data procedures should be in place in any location, call centre or office environment where confidential data is being processed and transferred or transmitted especially where the data is personal data or special category data or business sensitive.
- When choosing such an environment, the follow factors must be considered:
 - The office or workspace must be lockable and or accessible via a coded key pad (or similar device) and be accessible only to authorised staff;
 - If the office or workspace is sited on the ground floor, windows must be lockable and screens must be located so they cannot be seen by unauthorised personnel through the windows;
- Locked doors should not be propped open;
- Escort visitors and check they are authorised;
- Computers must not be left on view so that members of the general public or staff who do not have a justified need to view the information can see personal data;
- If moving away from a computer or laptop screen it must be locked. Select CONTROL + ALT + DELETE and ensure you hit the enter key. Or select the WINDOWS KEY + L to quickly lock a screen;
- If you see a colleague's device open and unlocked, lock it for them and remind them to do so in future.

- Computers or laptops must be switched off when not in use.
- Only Vocare approved encrypted laptops or desktops are to be used which include encryption software
- Information must be held on the secure network and not on desktops.
- Passwords must not be shared. Strong passwords must be used on all your devices to prevent unauthorised access. You should also use different passwords for each account. Creating strong passwords doesn't need to be a daunting task if you follow simple guidelines. The National Cyber Security Centre (NCSC) has a range of guidance on good password management, to help you set secure passwords: <https://ororwww.ncsc.gov.uk/blog-post/three-random-words-or-think-random-0>
- Manual paper records containing confidential data must be stored in locked cabinets when not in use and securely stored when the workstation is left unattended. Make sure you lock documents away if away from your desk during the day, evenings and weekends;
- Documents should not be left unattended for any significant period e.g. post should not be left unattended in post trays or on desks;
- Post trays should be situated away from any unauthorised access and situated where they can be monitored and mail must be disseminated to the addressee as soon as possible.

General principles of email usage

- All emails containing personal identifiable information must be sent to a secure address, i.e. nhs.net from an nhs.net account.
- If personal or sensitive data is to be sent, this should be sent from the individual nhs.uk account to the regional Governance Department who will send it to nominated nhs.net recipient via their own nhs.net account.
- No email containing identifiable or sensitive information must be sent to private email addresses including one's own.
- Never automatically "reply all"; always check all the email addresses are correct and it is appropriate that they are included in your response. If someone within the chain has made a mistake and you "reply all" you will be repeating the error and this could end in an unauthorised disclosure which could result in a CCG Data Security breach or IG Incident which may be reportable to the ICO. This could potentially result in a monetary fine and more importantly a loss of public trust.
- Always carefully check email addresses before you send an email. NHS Mail is a national system which contains similar email address for the same name.
- Always ensure you regularly review any distribution lists (DL) that you have created to ensure all the recipients are still current and correct.

The difference between “TO” “CC” and “BCC”

The consequences of not understanding the difference can be a data breach.

- TO is the person exactly to whom you are sending the email. Generally, the whole purpose of the email is to express or pass information to the person who is in the TO field.
- CC stands for Carbon Copy. When writing emails, the actual recipients address will be included in TO field of the mail application. People who are not directly involved or acting on the subject matter will be included in CC field for information purposes.
- BCC stands for Blind Carbon Copy, which is exactly similar to CC but the email addresses included in the BCC field will not be visible to anyone else other than the particular recipient. This function is particularly important where you wish to send an email to a distribution list without disclosing email addresses to other email recipients who do not need to know the email addresses of others.
- Emails which contain personal confidential data should always be appropriately titled i.e. do not include confidential details in the subject line such as name.
- If you do send an email in error, you can use the recall facility ‘recall this message’ (please note this function is only available in Outlook and not web-based NHS Mail). If the recipient hasn’t read the message it will be removed from their inbox. If they have opened the message a recall message will make them aware that the message was not meant for them and they may delete it, although they won’t be prompted to do so and may have already read the information.
- If you have sent an email containing personal data in error, you must report it immediately following the incident reporting procedures [Datix] and to the Data Protection Officer (DPO) and to Vocare’s national Quality Team so it can be investigated. For further information relating to incidents please follow the process documented within the V- IG 757 Information Governance related Serious Incidents Requiring Investigation (IG SIRI) Policy.
- Tidy up your contacts list and any distribution lists regularly to ensure out of date emails addresses do not pop up automatically and to ensure any leavers or authorised recipients are not included in the distribution list.
- Never disclose passwords or log on details to anyone, even a colleague, those details are private and must remain so.
- If you receive an unsolicited email containing an attachment or a link that you have not asked for do not open it or click on it as it as you could be subject to a phishing attack. This is where criminals or hackers sometimes use a link or attachment to install malicious software on your computer.
- Always check the recipients email address is correct before you press send.

Transfers of Data by Email from NHS Mail

- Personal data and or business sensitive data must always be sent via NHS Mail or an NHS approved encrypted email system. NHS Mail accounts have the suffix @nhs.net. (firstname.secondname@nhs.net), emails will be sent or received via the encrypted NHS Mail service.
- Please note NHS accounts which end in @nhs.uk may not be secure. If you are sending personal data and or business sensitive data and are unsure whether you are sending to an encrypted email account, always ask. This is even from an nduc.nhs.uk or vocare.nhs.uk email address.
- Organisations external to the NHS such as local authority, councils, local providers e.g. care homes have different email accounts. The list below states those non-NHS domains where emails can be sent to and from an NHS Mail account and it will be sent encrypted and therefore secure;
 - *.gcsx.gov.uk for local government
 - *.gsi.gov.uk and *.gsx.gov.uk for central government
 - *.cjsm.net and *.pnn.police.uk for Police or Criminal Justice
- When emailing personal data and or business sensitive data to outside third party organisations that do not have NHS Mail, they must have either an approved email encryption software (AES) system in place and or the NHS Mail process for sending emails securely to non NHS Mail accounts must be used.

NHS Mail process for sending emails securely to non NHS Mail accounts

NHS Mail users can now send encrypted and secure emails to non NHS Mail accounts (non-accredited or non-secure recipients) including Gmail, Hotmail etc..

When you enter [secure] in the subject line of the email and click send, the email is encrypted and protected with a digital signature on the NHS Mail platform within the UK. The recipient will be asked to authenticate to the service (they will receive an alert from the Trend Encryption Portal and be asked to 'Open Message' where they will need to enter their password).

The formatting of the message will be preserved, and attachments can be included. The sent item will be stored in your Sent Items folder, and any replies received will be decrypted and displayed as normal in NHS Mail. The recipient will be able to reply, forward the email on and it will still remain secure and encrypted.

For further details please refer to the NHS Mail Encryption Guide –You can access this on the link below:

<https://orors3-eu-west-1.amazonaws.com/orcomms-matorTrainingMaterials/orGuidance/encryptionguide.pdf>

<https://orors3-eu-west-1.amazonaws.com/orcomms/matorTrainingMaterials/orGuidance/orattachments/guide.pdf>

How to send an encrypted email from an NHS Mail account

- Using your NHS Mail account as normal, create a new message as normal
- Ensure the recipients email address is correct
- In the Subject field of the email, type the word [secure] before the subject of the message. The word secure must be surrounded by the square brackets for the message to be encrypted. If square brackets are not used, the content of the email will be sent in plain text and may potentially be exposed to interception or amendment
- Type your message
- Send the email as normal Note: [secure] is not case sensitive and [SECURE] or [Secure] for example could also be used.

NHS Digital Secure Email Standard

- Various organisations are looking at achieving NHS Digital Secure Email Standard (DCB1596), meaning once achieved the organisation will be able to email securely from their email accounts. Organisations looking to become accredited are required to undergo a vigorous assessment by NHS Digital and once passed they receive a Conformance statement for NHSmail. This would mean you would not need to use the [secure] method and the organisation could email to your NHSmail account (and vice a versa) as normal, as you do with NHSmail colleagues.
- You will notice that these organisations who have NHS Digital Secure Email Standard will still keep their email addresses ending in co.uk, nhs.uk etc.

Use of Vocare or Totally plc accounts

- Any information sent within and between these two systems are considered to be secure.

Telephone Disclosures

There will be occasions when telephone enquiries are received asking for disclosure of personal data. When the disclosure is legally justified and the caller has a legal right to access that information, the following rules should be adhered to:

- Verify personal details including the name, job title and organisation of the person requesting information;
- Obtain and record enquiries telephone number;

- If the caller is part of an organisation the main switchboard number of that organisation (via phone book or directory enquiries) should be obtained and ring back;
 - Conduct the call in an area that is private and confidential where staff or public cannot overhear. Any notes made during the calls should be kept in a secure place (locked away) and not left on any desk;
 - If in doubt, the caller should be advised that they will be called back and where necessary, a senior manager or the designated authority for confidentiality issues should be consulted;
 - Any suspect or bogus enquiries should be referred immediately to the DPO, SIRO or IG Team as soon as possible and an incident logged;
 - Always provide the minimum amount of information that is necessary;
 - Provide the information only to the person who requested it and do not leave a message;
- Be aware of any press enquiries and immediately refer to the Vocare national Quality Team

Transfers of Data by Post

The following rules must be followed when sending or receiving personal data via post:

Incoming:

- Ensure incoming post is received in an environment away from unauthorised public interference e.g. not left on desks or in a waiting or public area;
- Open incoming mail away from public areas;
- Ensure if post is sorted for onward distribution that it is stored securely prior to dissemination and regular deliveries are made so there is no delay in receipt of the information for the receiver and is picked up frequently.

Outgoing:

- Check if you need to use a courier or “signed for” Royal Mail service to post to ensure receipt of delivery;
- Always double check the contact details and address of the recipient or the recipient’s representative;
- Ensure the recipient’s contact details are clearly labelled on the envelope or package;
- If the envelope contains confidential data, mark the envelope clearly as ‘Private and confidential’;
- Use a Vocare letter headed front page or compliment slip;
- Use a secure robust envelope, include a return address where appropriate;
- For important letters or parcels, ask for confirmation of safe arrival.

Manual transfers of Paper

- Paper records, documents and hard copies of electronic information may be required for investigation or to refer to as part of patient care. The following rules must be followed regarding confidential paper

documentation:

- Paper documents that contain confidential information must be stored in a lockable cupboard or cabinet prior to sending (if they have to be stored);
- Lockable cases must be used to move bulk hardcopy information;
- Only take off site the minimum amount of paper documentation that is necessary
- Record what paper documentation is taken off site, particularly if this is patient information, where and whom the information has gone to
- Never leave personal, sensitive or confidential records unattended – ensure they are always stored securely when not required;
- If you no longer need the paper documentation, ensure this is confidential disposed of using the Vocare confidential shredding process.

Transfers of Data via Text Message

Text messaging is becoming increasingly popular between staff. The following must be considered before any text messages are used:

- Check the mobile number is correct and be confident that the person using the recipient's mobile is the person to whom the message is intended;
- Keep messages short;
- Do not transfer business sensitive or personal confidential data via text;
- Mobile phone networks may be open to additional risks of eaves dropping or interception;
- Remember data sent via text message could be released via a Freedom of Information request and or a subject access request.

Transfers of Data using Portable Devices

- The use of portable devices such as laptops, mobile phones, smartphones, tablets, USB memory sticks to transfer and store information for work purposes must be in line with Vocare's policy and authorised by your line manager
- Only portable devices that are approved by Vocare and are encrypted to NHS standards and where appropriate have up to date anti-virus software can be used for work purposes to transfer data with and or store data.
- Personally-owned portable devices such as laptops, smart phones, tablet devices must not contain work related information or information assets and must not be directly connected to the corporate network either by a direct network cable connection or Wi-Fi connection. However, such devices may be

connected to the Vocare 'guest' Wi-Fi service but only if in accordance with Vocare's Digital, Data Security and Information governance policies and procedures.

- Data on laptops must always be stored on the secure network folders. When off site, you can access this via VPN or remote access token. Never store data on the local drive of a laptop, this is insecure.
- In order to be issued with a portable device a member of staff must complete the required approval forms and have it authorised by their Line Manager.
- All security and encryption features on portable devices must be utilised such as username and password authentication. Where additional safeguards can be put in place, they must be done so such as a minimum 4 digit PIN being allocated to a mobile phone.
- For any issues related to use of the portable device such as malfunction, staff members should contact Digital Services.
- When staff leave Vocare they must return any equipment provided by the organisation.

Transfers of Data by the NHS Secure Electronic File Transfer (SEFT)

- Service Secure Electronic File Transfer (SEFT) works by providing a secure wrapper around any file, regardless of its size, structure or data content. SEFT provides data security during transmission, by using a 256-bit AES encryption mechanism. The data are held in secure containers at NHS Digital and only people who are authorised to process the data are allowed access.
- SEFT can only be accessed by registered and approved users. Further information can be found on the link below: <https://digital.nhs.uk/services/transfer-data-securely>.

Transfers of Data via Social Media Platforms

Transfers of business confidential information or personal data to social media platforms is not permitted.

Only approved information by Vocare/totally is published on social media platforms such as Twitter and Facebook. These platforms must not be used to transfer or store business information or to discuss any work-related issues.

Transfers of Data via Audio Recordings

- **Meeting recordings** - the recording of audio is a useful tool to record an event, such as, to record minutes of a meeting. If any meetings are to be recorded, then only approved Vocare equipment must be used and those in attendance at the meeting must be informed. The recording must be deleted from the audio recording device as soon as practicable and the device must always be locked away when not in use.

- **Call recordings** - may be sent to recipients as part of an investigation or complaint. These will be sent via encrypted memory stick or by encrypted email attachments.
- **Call reviews** - are sent from the NHS.net email to NHS.net recipients. In the rare instance that a recipient has no NHS.net email account, the call audits are sent on an encrypted memory stick.

Transfers of data via photography and video equipment

Use of digital photography and video recording provide a permanent record of an event for a range of different purposes, such as outreach work. Such devices rarely contain the ability to encrypt images stored on the device. As a result, there is a risk of unauthorised access if the device, or a removable memory card, is lost or stolen.

Therefore, it is important that images, recordings from a camera or recording device are transferred to a secure location and the remaining content deleted from the memory card and device as soon as is practical.

Transfer of Data Overseas

If there are any occasions when you need to transfer business sensitive, personal confidential data overseas, always seek the advice from the Data Protection Officer or the Vocare national Quality Team first. The security of the transfer and the recipient arrangements for security must be checked prior to any transfers being made. Please refer to the V-IG P42 Transfer of Data outside the European Economic Area [EEA] policy.

Disposal and Deletion of Data.

All users must ensure that, where equipment is being disposed of, all data on the equipment or device is securely destroyed following the V-IG 976 Records Retention Policy. Any paper documentation that is no longer required following transfer must either be filed away securely or securely disposed of using the confidential waste bins. When staff use portable devices to transfer or temporarily store data, for example, via USB devices, the data must be deleted as soon as no longer required.

10. Data Breaches within this Process

If you have sent any information containing personal data that falls outside these processes, you must report it immediately following the incident reporting procedures (Datix) to the Data Protection Officer (DPO) and to the Vocare national Quality Team so it can be investigated. For further information relating to incidents please follow the process documented within the V- IG 757 Information Governance related Serious Incidents Requiring Investigation (IG SIRI) Policy.

11. Involvement of External Partners

Breaches of these processes may be reported to NHS Digital, who may on refer to the Information Commissioners' Office. It may also be necessary to inform the Care Quality Commission. Consideration must be given to the importance of the organisation's legal responsibilities towards duty of candour and inform data subjects if their confidentiality has been breached.

12. Escalation to the Data Protection Officer and to the Caldicott Guardian

Once reported on Datix, escalation to the DPO and Caldicott Guardian will be undertaken by the Head of Clinical Governance.

13. Governance

The governance for this policy will be overseen by the Director of Corporate Assurance.

14. Related Policies and Standard Operating Procedures

[V-IG 757 IG Related Serious Incident Policy V1.01](#)

[V-IG 966 Data Protection GDPR V1.01](#)

[V-IG 972 Information Security Handbook V1.00](#)

[GDPR Rollfold V1.00 2019](#)

[V-IG 994 Appropriate Use of Email V1.00](#)

[V-IG 976 Records Retention Policy V1.00](#)

[V-IG 971 Information Security Breach Process V1.00](#)

[V-IG 963 Clear Desk Clear Screen V1.01](#)

[V-IG 992 Information Security Policy V1.00](#)