Trust Standard Operating Procedure

University Hospitals Plymouth NHS Trust

Disclosure of Personal Information by Email SOP

Issue Date	Review Date	Version
July 2018	July 2023	2

Purpose

To provide staff with information regarding use of email when disclosing personal data relating to patients or staff.

Who should read this document?

All staff who handle confidential information relating to patients and/or staff.

Key Messages

This procedure provides staff with general principles to follow when disclosing personal data by email as well as information on:

- Secure Email Address
- NHSMail Encryption
- Emailing Patients

Core accountabilities	
Owner	Information Governance Support Manager
Review	Caldicott and Information Governance Assurance Committee
Ratification	Senior Information Risk Owner
Dissemination	Information Governance Support Manager
Compliance	Information Governance Support Manager

Links to other policies and procedures

Information Governance Policy
Information Security Policy

Version History

V1	March 2016	Creation of document following archive of APN – Disclosing Information by Email
V1.1	December 2016	Minor amendments of secure email addresses
V1.2	July 2017	Process amendments made following document consultation
V1.3	November 2017	Further review following introduction of pilot
V2	July 2018	Review in line with new Data Protection legislation and amendment to process

The Trust is committed to creating a fully inclusive and accessible service. Making equality and diversity an integral part of the business will enable us to enhance the services we deliver and better meet the needs of patients and staff. We will treat people with dignity and respect, promote equality and diversity and eliminate all forms of discrimination, regardless of (but not limited to) age, disability, gender reassignment, race, religion or belief, sex, sexual orientation, marriage/civil partnership and pregnancy/maternity.

An electronic version of this document is available on Trust Documents on StaffNET. Larger text, Braille and Audio versions can be made available upon request.

Standard Operating Procedures are designed to promote consistency in delivery, to the required quality standards, across the Trust. They should be regarded as a key element of the training provision for staff to help them to deliver their roles and responsibilities.

Plymouth Hospitals NHS
NHS Trust

Standard Operating Procedure (SOP)

Disclosure of Personal Information by Email

1 Introduction

This procedure is designed to provide general advice to staff in respect of disclosing personal data via email in order to minimise and eliminate risks of inappropriate disclosure.

There may be circumstances that are not covered by this procedure as it cannot describe exact action to take in every eventuality, however staff should abide by the general principles outlined within this document to protect patient/staff confidentiality.

This procedure does not include whether or not a particular piece of information can be disclosed. For this to be determined, staff should familiarise themselves with the relevant legislation or regulations.

Staff need to appropriately balance maintaining patient confidentiality against patient care at all times.

2 Definitions

Personal Data

This is information which relates to an individual (including patients and staff) who can be identified from that information. Consideration must be given to the combination of this and any other information coming into the possession of the holder of that data which will allow for identification.

3 Regulatory Background

Data Protection Law

The Data Protection Act 2018 and EU General Data Protection Regulation (GDPR) covers the way organisations process personal data of living individuals.

Common Law Duty of Confidentiality

Information is only disclosed to individuals who are authorised to receive it by individuals who are authorised to release it. Disclosure is determined on a need to know basis.

Caldicott Report

The seven Caldicott Principles when using patient information are:

- Justify the purpose
- Only use if absolutely necessary
- Use the minimum required
- Access on a need to know basis
- Everyone must understand their responsibilities
- Understand and comply with the law
- The duty to share information can be as important as the duty to protect confidentiality.

4 Key Duties

All staff have a duty to protect patient/staff confidentiality in line with the relevant legislation. This procedure is designed to help staff maintain their obligations.

5 Procedure to Follow

The Trust uses NHSmail as its primary email service which is secure for the transmission of person identifiable information relating to patients or staff between other NHSmail users.

Guidance for NHSmail: https://portal.nhs.net/Help/policyandguidance

5.1 Secure Email Addresses

Transmitting person identifiable information by email is a preferred method of communication within the NHS as long as it is carried out securely i.e. @nhs.net to @nhs.net.

Information should be restricted to the minimum that is necessary and strictly only sent to those staff that have a specific need to know.

Personal data should not be circulated to large distribution lists unless each staff member has a definite need to know. For example, emails regarding missing casenotes sent to the PHNT Noticeboard should be restricted to initials and hospital number only.

5.2 NHSmail Encryption

If sending person identifiable data by email from NHSmail to a non NHSmail email address then NHSmail encryption **must** be used.

See the user guide for further information:

http://nww.plymouthict.nhs.uk/HelpGuidance/NHSmailencryption.aspx

5.3 Emailing Patients

Many patients request communication by email. Sending emails outside NHSmail such as to email addresses ending @hotmail.com, @google.com etc without NHSmail encryption is **not** secure.

The Trust does not rely on emailing patients as the preferred method of communication. However, if a staff member or patient wishes to correspond by email then the patient should acknowledge the Email Privacy Notice available in Organisational Forms on Microsoft Outlook.

Emails should be filed in the patient's health record.

6 Document Ratification Process

The design and process of review and revision of this procedural document will comply with The Development and Management of Formal Documents.

The review period for this document is set as default of five years from the date it was last ratified, or earlier if developments within or external to the Trust indicate the need for a significant revision to the procedures described.

This document will be reviewed by the Caldicott and Information Governance Assurance Committee and ratified by the Senior Information Risk Owner.

Non-significant amendments to this document may be made, under delegated authority from the Senior Information Risk Owner, by the nominated author. These must be ratified by the Senior Information Risk Owner and should be reported, retrospectively, to the Caldicott and Information Governance Assurance Committee.

Significant reviews and revisions to this document will include a consultation with named groups, or grades across the Trust. For non-significant amendments, informal consultation will be restricted to named groups, or grades who are directly affected by the proposed changes.

7 Dissemination and Implementation

Following approval and ratification, this procedural document will be published in the Trust's formal documents library and all staff will be notified through the Trust's normal notification process, currently the 'Vital Signs' electronic newsletter.

Document control arrangements will be in accordance with The Development and Management of Formal Documents.

The document author(s) will be responsible for agreeing the training requirements associated with the newly ratified document with the Senior Information Risk Owner and for working with the Trust's training function, if required, to arrange for the required training to be delivered.

8 Monitoring and Assurance

This procedure is underpinned by the Information Governance Policy.

All breaches of confidentiality must be reported on the Trust Incident Reporting System, Datix. Staff should also notify their Line Manager and the Information Governance Team.

Staff that breach confidentiality may be subject to disciplinary action in line with the Trust Performance and Conduct Policy.

9 Reference Material

Data Protection Act (2018)
https://www.gov.uk/data-protection

EU General Data Protection Regulation
http://www.eugdpr.org/

Caldicott Report
http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4068403

Confidentiality: NHS Code of Practice DoH (2003)
http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4069253