Trust Policy

University Hospitals Plymouth NHS Trust

Electronic Signature Policy

Issue Date	Review Date	Version
October 2020	October 2025	1

Purpose

This policy is concerned with use of electronic signatures. These can exist in many different forms and not just as digital images of hand-written signatures.

The policy is to ensure that any individual or the Trust:

- is not misrepresented;
- does not suffers loss of reputation;
- is not exposed to any liability or other adverse consequence through the unauthorised use of electronic signatures.

Following the requirements of this policy is essential and any breach may lead to disciplinary action being taken. Such a breach may result in summary dismissal.

Who should read this document?

This policy and associated procedures is targeted at all personnel who may act in some capacity as signatories on behalf of the Trust.

Key Messages

The Trust has a duty to meet local and national requirements in relation to the security and integrity of information. As the Trust requires electronic signatures which can be used in place of written signatures in order to increase the efficiency of its business processes, it is important that they fulfil the same functions as written signatures and provide the appropriate levels of authentication, integrity and non-repudiation to a document.

This policy sets out the functional requirements for electronic signatures and defines acceptable uses of electronic signatures for signing documents, electronically as an equivalent to a hand written signature.

Core accountabilities	
Owner	Dr Chris Rollinson, Research Governance Manager
Review	Caldicott and Information Governance Assurance Committee (CIGAC)
Ratification	Lee Budge, Director of Corporate Business
Dissemination (Raising Awareness)	Caldicott and Information Governance Assurance Committee (CIGAC)
Compliance	Dr Chris Rollinson, Research Governance Manager

Links to other policies and procedures
Counter Fraud Policy

Version History		
1	October 2020	Final Version approved by CIGAC

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. Larger text, Braille and Audio versions can be made available upon request.

Contents

Contents

1. Introduction

Manual signatures can be captured by various types of equipment including scanners, photocopiers and mobile phones. Once acquired, signatures can be transmitted electronically and copied between files, as well as being printed on paper documents.

An electronic document, such as an email or Word file, containing a digitised signature is nowadays considered to be no different from a paper one which has been signed manually.

It is therefore important that individuals use images of their own signatures with care and that there are controls over the use of other people's digitised signatures.

From a legal perspective there is normally no need to include an image of a signature in a document. The (typed) text at the end of an email acts as a signature if it meets the requirements in section 3, (a) and (b) below. This applies to standard Trust emails.

2. Purpose and Scope

This policy applies to all full time and part time employees on a permanent or fixed term contract, and to associated persons working for the Trust such as secondees, agency staff, contractors and others employed under a contract of service.

3. Definitions

Electronic signature. The legal definition of an "electronic signature" is anything in electronic form which is:

(a) Incorporated into or otherwise logically associated with any electronic communication or electronic data; and

(b) Purports to be so incorporated or associated for the purpose of being used in establishing the authenticity of a communication or data, the integrity of the communication or data, or both. *Electronic Communications Act 2000 and Electronic Signatures Regulations 2002.*

Non repudiation. In reference to digital security, non-repudiation means to ensure that a transferred message has been sent and received by the parties claiming to have sent and received the message. Non repudiation is a way to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message.

4. Duties

4.1 Accountable Officer

The Accountable Officer has overall responsibility for ensuring that information is handled appropriately in order to protect information from unauthorised disclosure or misuse. This role is carried out by the Director of Corporate Business as the Trust's Senior Information Risk Owner (SIRO).

4.2 Line Managers

Line Managers have a responsibility to:

- Develop and support the implementation of the Policy and ensure the Trust meets national and local requirements.

4.3 All staff

All staff have a responsibility to:

- Make themselves familiar with and adhere to this Policy. Failure to comply may result in disciplinary action being taken.
- Bring to managers' attention areas of concern regarding any issues associated with use of electronic signatures.
- Seek advice from the IM&T Information Security Officer as necessary.
- Co-operate with the development and implementation of policies and procedures and as part of their normal duties and responsibilities.
- Identify the need for a change in policy or procedure as a result of becoming aware of changes in practice, changes to statutory requirements, revised professional or clinical standards and local/national directives, and advising their line manager accordingly.
- Identify training needs in respect of policies and procedures and bringing them to the attention of their line manager.
- Attending training / awareness sessions when provided.
- Where signatories are to be inserted as 'on behalf of', authorisation should be obtained in writing[1], in advance, from the main signatory. This may be in the form of a general delegation of authority or a specific delegation covering a single instance. Verbal approval should be followed up by written approval as soon as possible. In exceptional circumstances, where time is of the essence, (including annual leave), per procurationem (p.p.) signatures may be added without explicit

permission. As a minimum, the main signatory must be copied into the document, who should acknowledge receipt.

- To report any concerns regarding the misuse of electronic signature

5. Main Body of Policy

5.1 The function of a signature

A signature is only as good as the business process and technology used to create it[1]. Any electronic signatures used therefore must meet the functional requirements needed from a signature in the business process. Staff implementing electronic signatures must ensure that the appropriate form of electronic signature is used to meet the requirements. The functional requirements of a signature include:

- confirming originality and authenticity of a document;
- demonstrating a document has not been altered;
- indicating a signer's understanding and/or approval;
- indicating a signer's authorisation;
- identifying the signatory and ensuring non-repudiation of a document.

[1] Department for Business Enterprise & Regulatory Reform Electronic Signatures and Associated Legislation (2009) p.1

5.2 Types of Electronic Signatures

5.2.1. Electronic signatures can be divided into three groups:

1. **Simple electronic signatures** – examples are a stylus or finger drawn signature, a typed name, a tick box and declaration, a unique representation of characters, scanned image of a signature and an automatic e-mail signature.
2. **Advanced electronic signatures** – these are uniquely linked to the signatory, are capable of identifying the signatory, allow the signatory to retain control, and are linked to data within the signature that can detect any changes made.
3. **Qualified electronic signatures** – an advanced electronic signature, uniquely linked to the signatory, that is created by a qualified electronic signature creation device, and which is based on a qualified certificate for electronic signatures.

The use of 'advanced' or 'qualified' electronic signatures provides:

a. Authentication – the signatory can be linked to the information

b. Integrity – changes to the information can be detected more easily.

c. Non-repudiation – legal assurance regarding where the electronic signature has come from.

5.2.2. Examples of Electronic Signatures

DocuSign (https://www.docusign.com/why-docusign), SigningHub (https://www.signinghub.com/security/advanced-electronic-signatures/) and Adobe (https://helpx.adobe.com/acrobat/kb/certificate-signatures.html) are examples of companies which can deliver all of the signature types defined under the eIDAS regulation, including EU Advanced and EU Qualified electronic signatures.

It is important to remember that any type of electronic signature is admissible as court evidence by virtue of the 'eIDAS' Regulation, however, some are more reliable and carry greater evidential weight and assurance than others, as described above.

5.3 Requirements

5.3.1. Scanned image of a handwritten signature

As is current practice, a scanned image of a handwritten signature can be used as an equivalent to a written signature where it meets the appropriate functional requirements.

Scanned images must only be used where express permission has been granted by the author and are therefore more likely to be acceptable for high volume processes such as mass mailings.

Scanned images of signatures must be kept securely to prevent unauthorised access and fraudulent use.

Responsibility for authorisations made by scanned signature remains with the signature's author however the author will not be held responsible for any malicious, fraudulent or negligent activity carried out by the proxy.

Images of signatures should be used only when essential.

Though it is only a small deterrent to copying images of signatures, they should be sent outside the organisation in PDF files rather than emails, Word documents or spreadsheets. The PDF files should be created with the highest levels of protection.

Documents containing the image of another person's signature must not be sent without the express agreement of the person concerned, unless prior delegation and clearance procedures have been agreed. In addition:

- such agreement, including the list of recipients, must be obtained in advance for each document.
- the content of the document must not be changed after authorisation to issue it has been obtained.
- once such a document has been sent, it must not be sent again (or to additional recipients) without further explicit authorisation.

5.3.2. Authorisation by email

An email from an individual user's NHS.net e-mail address can be used as an equivalent to a written signature for internal purposes where it meets the appropriate functional requirements.

Responsibility for authorisations made by email remains with the email account holder unless the proxy is acting maliciously, fraudulently or negligently or unauthorised access to the account has been obtained in breach of the Computer Misuse Act 1990.

5.3.3. Advance or qualified electronic signatures

Advance or qualified signatures may be required by third parties when greater assurance is required particularly for contractual signatures.

5.4 Legal Impact of Electronic Signatures

- it is possible to commit to contracts using electronic signatures
- An electronic signature could be used in court as evidence of the Authenticity of the communication or document if it is separately confirmed that the signature is

a means of authenticating the communication or document. (Section 7 of the Electronic Communications Act 2000).

5.5 Precautionary Measures

- It should be noted that it is possible for e-mails to be “spoofed” or “hijacked” i.e. appear to be sent by someone other than the true sender, and for this reason a degree of caution needs to be exercised when accepting e-mails from third parties. Check the actual email address of the sender to help identify whether it is correct. If there is any doubt as to the authenticity of an electronic communication, it should in the first instance be reported to the IM&T Information Security Officer for further investigation.

5.6 Related Policies

As stated in the Trust’s Internet Use, NHSmail Acceptable Use, Network Security, Email, Computers and Telecommunications policies: "User-ids and passwords must be kept confidential, and never displayed, shared, or saved for automatic connection".

It is not acceptable to send an email logged on as another person. Both disclosure of a personal password and use of another person's password are potentially serious disciplinary offences.

6. Overall Responsibility for the Document

The Senior Information Risk Owner (SIRO) is responsible for ensuring compliance with this policy. The Director of Corporate Business is designated in this role.

7. Consultation and Ratification

The design and process of review and revision of this policy 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 senior management team and ratified by the Director of Corporate Business.

Non-significant amendments to this document may be made, under delegated authority of the nominated owner. These must be ratified by the Director of Corporate Business.

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 that are directly affected by the proposed changes.

8. Dissemination and Implementation

Following approval and ratification, this policy will be published in the Trust's formal documents library and all staff will be notified through the Trust's normal notification process.

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

The document owner will be responsible for agreeing the training requirements associated with the newly ratified document with the named Director and for working with the Trust's training function, if required, to arrange for the required training to be delivered.

9. Monitoring Compliance and Effectiveness

The Governing Body will agree a method for monitoring the dissemination and implementation of this policy. Monitoring information will be recorded in the policy database.

10. References and Associated Documentation

Electronic Communications Act 2000 and Electronic Signatures Regulations 2002

eIDAS Regulation: Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market. Effective on 1st July 2016 as a European Regulation and automatically applies in the UK. (There are also some specific provisions on its effect, supervision and enforcement in the UK set out in the Electronic Identification and Trust Services for Electronic Transactions Regulations 2016 (the UK eIDAS Regulations).

Computer Misuse Act 1990

Dissemination Plan and Review Checklist | Appendix 1

Dissemination Plan	
Document Title	Electronic Signature Policy
Date Finalised	16th Oct 2020
Previous Documents	
Action to retrieve old copies	N/A

Dissemination Plan

Recipient(s)	When	How	Responsibility
All Trust staff		IG StaffNet Page	Information Governance Team

Review Checklist		
Title	Is the title clear and unambiguous?	✓
	Is it clear whether the document is a policy, procedure, protocol, framework, APN or SOP?	✓
	Does the style & format comply?	✓
Rationale	Are reasons for development of the document stated?	✓
Development Process	Is the method described in brief?	✓
	Are people involved in the development identified?	✓
	Has a reasonable attempt has been made to ensure relevant expertise has been used?	✓
	Is there evidence of consultation with stakeholders and users?	✓
Content	Is the objective of the document clear?	✓
	Is the target population clear and unambiguous?	✓
	Are the intended outcomes described?	✓
	Are the statements clear and unambiguous?	✓
Evidence Base	Is the type of evidence to support the document identified explicitly?	✓
	Are key references cited and in full?	✓
	Are supporting documents referenced?	✓
Approval	Does the document identify which committee/group will review it?	✓
	If appropriate have the joint Human Resources/staff side committee (or equivalent) approved the document?	✓
	Does the document identify which Executive Director will ratify it?	✓
Dissemination & Implementation	Is there an outline/plan to identify how this will be done?	✓
	Does the plan include the necessary training/support to ensure compliance?	NA
Document Control	Does the document identify where it will be held?	✓
	Have archiving arrangements for superseded documents been addressed?	NA
Monitoring Compliance & Effectiveness	Are there measurable standards or KPIs to support the monitoring of compliance with and effectiveness of the document?	NA
	Is there a plan to review or audit compliance with the document?	NA
Review Date	Is the review date identified?	✓
	Is the frequency of review identified? If so is it acceptable?	✓
Overall Responsibility	Is it clear who will be responsible for co-ordinating the dissemination, implementation and review of the document?	✓

Equalities and Human Rights Impact Assessment | Appendix 2

Core Information	
Date	19th Oct 2020
Title	Electronic Signature Policy
What are the aims, objectives & projected outcomes?	This policy is concerned with use of electronic signatures. These can exist in many different forms and not just as digital images of hand-written signatures. The policy is to ensure that any individual or the Trust: is not misrepresented; does not suffers loss of reputation; is not exposed to any liability or other adverse consequence through the unauthorised use of electronic signatures.
Scope of the assessment	
Collecting data	
Race	
Religion	
Disability	
Sex	
Gender Identity	
Sexual Orientation	
Age	
Socio-Economic	
Human Rights	
What are the overall trends/patterns in the above data?	
Specific issues and data gaps that may need to be addressed through consultation or further research	

Involving and consulting stakeholders	
Internal involvement and consultation	
External involvement and consultation	
Impact Assessment	
Overall assessment and analysis of the evidence	

Action Plan				
Action	**Owner**	**Risks**	**Completion Date**	**Progress update**