

Corporate	CCG CO27 Electronic Signature
------------------	--------------------------------------

Version Number	Date Issued	Review Date
V1	November 2020	November 2022

Prepared By:	Senior Governance Manager, North of England Commissioning Support
Consultation Process:	NT CCG Director of Contracting & Finance NT CCG Senior Provider Management Lead
Formally Approved:	Governing Body; 24 November 2020

Policy Adopted From:	CO26: Electronic Signature Policy (1); NHS County Durham CCG
-----------------------------	--

DOCUMENT HISTORY

Version	Date	Significant Changes
1	November 2020	First Issue

EQUALITY IMPACT ASSESSMENT

Date	Issues
September 2020	Section 11. No issues identified.

POLICY VALIDITY STATEMENT

Policy users should ensure that they are consulting the currently valid version of the documentation. The policy will remain valid, including during its period of review. However, the policy must be reviewed at least once in every 3 year period.

ACCESSIBLE INFORMATION STANDARD STATEMENT

If you require this document in an alternative format such as easy read, large text, braille or an alternative language please contact NECSU.comms@nhs.net

Version Control

Version	Release Date	Author	Update comments
V1	November 2020	NECS Senior Governance Manager, NECS	Adopted from NHS County Durham CCG. Minor adaptations for North Tyneside CCG e.g. job titles.

Approval

Role	Name	Date
Approval	Governing Body	November 2020

Contents

1. Introduction	4
2. Definitions	5
3. The function of a signature.....	6
4. Requirements.....	6
5. Incident Reporting.....	8
6. Implementation and Distribution.....	8
7. Training Implications	8
8. Documentation	8
9. References.....	8
10. Monitoring, Review and Archiving	9
11. Equality Analysis	10
Appendix A Duties and Responsibilities	13

1. Introduction

NHS North Tyneside Clinical Commissioning Group (CCG) aspires to the highest standards of corporate behaviour and clinical competence, to ensure that safe, fair and equitable procedures are applied to all organisational transactions, including relationships with patients their carers, public, staff, stakeholders and the use of public resources. In order to provide clear and consistent guidance, the CCG will develop documents to fulfil all statutory, organisational and best practice requirements and support the principles of equal opportunity for all.

This document sets out the principles of the Electronic Signature Policy for North Tyneside CCG.

The CCG has a duty to meet local and national requirements in relation to the security and integrity of information. As the CCG 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.

1.1. Status

This policy is an Corporate policy.

1.2. Background, Purpose and scope

1.2.1 Background

Manual signatures can be captured by various types of equipment including scanners and photocopiers. 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 above. However electronic signatures should not be used in transactions where there is a legal requirement for a written signature (i.e. ink).

1.2.2 Purpose

To provide guidance to CCG staff on the use of electronic signatures and to ensure that neither the CCG nor any individual:

- is misrepresented;
- suffers loss of reputation;
- is 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 or legal proceedings, for example where a signature has been used fraudulently.

1.2.3 Scope

This policy applies to those members of staff that are employed, either permanently or temporarily, by the CCG and for whom the CCG has legal responsibility.

This policy sets out when electronic signatures will be acceptable for internal processes and the necessary supporting conditions. Electronic signatures may be used to make agreements with third parties where this is acceptable to the third party and appropriate.

2. Definitions

The following terms are used in this document:

2.1 Electronic Signature

The Electronic Communications Act 2000 and Electronic Signatures Regulations 2002 defines it as:

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.

It also states, "Electronic signature" means "data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication". This may include a scanned image of a handwritten signature, a typewritten signature in an email or a ticked box on an electronic form.

For the CCG this means that an email address, any email sent with a typewritten signature or automatic email signature, any scanned image of a handwritten signature or a ticked box on an electronic form will be classed as an electronic signature.

Digital signatures, which use cryptographic techniques and protect an entire document by detecting any change at all after "signature", are not covered by this policy.

The following are all examples of an electronic signature

- Typed name
- E-mail address
- Scanned image of a signature
- Automatic e-mail signature

2.2 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.

3. The function of a signature

A signature is only as good as the business process and technology used to create it¹. 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.

4. Requirements

Images of signatures should be used only where a clear audit trail of authorisation including written permission has been granted by the signatory. 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.

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

Documents containing the image of another person's signature must not be sent without a clear audit trail of authorisation including written permission of the person concerned, unless prior delegation and clearance procedures have been agreed. In such cases:

- 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.

All staff who allow a proxy to access their email account or scanned signature must ensure that the proxy is informed of the limits of their authority in the sending of emails or signing documents on behalf of the member of staff.

Electronic signatures should not be used in transactions where there is a legal requirement for a written signature, for example in the signing of a deed or other document where the signature is required to be witnessed.

Responsibility for authorisations made by email remains with the email account holder however the account holder will not be held responsible for any malicious, fraudulent or negligent activity carried out by the proxy.

The selection of an 'I agree' option (e.g. tick box or button) on an electronic form can be used as an equivalent to a written signature for internal purposes where it meets the appropriate functional requirements and the technology used records that the form has been signed and clearly identifies (e.g. by recording the username) the person who has 'signed' the form in this manner. The audit trail recording that the form has been signed and the signatory's identity must be accessible for the length of the retention period required for the form.

If the contents of a document change then the signature will be invalidated and a new signature sought.

The person signing the form should be able to access a copy of the submitted signed form for as long as it is required for reference purposes.

4.1 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 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.

5. Incident Reporting

Incidents may be reported by any member of staff where they feel that there is a mis-use of an electronic signature. Incidents are to be reported to the line manager, escalating to the relevant director as appropriate.

Examples of incidents are:

- Misuse of electronic signature, such as the use of somebody else's electronic signature purporting to be that other person
- Non-compliance to this Policy

6. Implementation and Distribution

This policy is available for all staff to access via the Intranet.

All directors and managers are responsible for ensuring that relevant staff within their own directorates and departments have read and understood this document and are competent to carry out their duties in accordance with the procedures described.

Line managers have a role to play in ensuring staff are aware of this policy and its implications.

7. Training Implications

No specific training requirements in relation to this policy have been identified.

8. Documentation

NHS England Tackling Fraud, Bribery and Corruption: Policy and Procedures

9. References

The major references consulted in preparing this document are described below.

Electronic Communications Act 2000 and Electronic Signatures Regulations 2002

10. Monitoring, Review and Archiving

10.1 Monitoring

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.

10.2 Review

The Governing Body will ensure that this policy document is reviewed in accordance with the timescale specified at the time of approval. No policy or procedure will remain operational for a period exceeding three years without a review taking place.

Staff who become aware of any change which may affect a policy should advise their line manager as soon as possible. The Governing Body will then consider the need to review the policy or procedure outside of the agreed timescale for revision.

For ease of reference for reviewers or approval bodies, changes should be noted in the 'document history' table on the front page of this document.

NB: If the review consists of a change to an appendix or procedure document, approval may be given by the sponsor director and a revised document may be issued. Review to the main body of the policy must always follow the original approval process.

10.3 Archiving

The Governing Body will ensure that archived copies of superseded policy documents are retained in accordance with Records Management: NHS Code of Practice 2016.

11. Equality Analysis

Initial Screening Assessment (STEP 1)

As a public body organisation we need to ensure that all our current and proposed strategies, policies, services and functions, have given proper consideration to equality, diversity and inclusion, do not aid barriers to access or generate discrimination against any protected groups under the Equality Act 2010 (Age, Disability, Gender Reassignment, Pregnancy and Maternity, Race, Religion/Belief, Sex, Sexual Orientation, Marriage and Civil Partnership).

This screening determines relevance for all new and revised strategies, policies, projects, service reviews and functions.

Completed at the earliest opportunity it will help to determine:

- The relevance of proposals and decisions to equality, diversity, cohesion and integration.
- Whether or not equality and diversity is being/has already been considered for due regard to the Equality Act 2010 and the Public Sector Equality Duty (PSED).
- Whether or not it is necessary to carry out a full Equality Impact Assessment.

Name(s) and role(s) of person completing this assessment:

Name: Aimee Tunney

Job Title: Governance & Assurance Manager

Organisation: North of England Commissioning Support Unit

Title of the service/project or policy: Electronic Signature Policy

Is this a;

Strategy / Policy

Service Review

Project

Other Not applicable

What are the aim(s) and objectives of the service, project or policy:

The CCG has a duty to meet local and national requirements in relation to the security and integrity of information. As the CCG 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.

Who will the project/service /policy / decision impact?

(Consider the actual and potential impact)

- **Staff**
- **Service User / Patients**
- **Other Public Sector Organisations**
- **Voluntary / Community groups / Trade Unions**
- **Others, please specify** [Click here to enter text.](#)

Questions	Yes	No
Could there be an existing or potential negative impact on any of the protected characteristic groups?	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Has there been or likely to be any staff/patient/public concerns?	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Could this piece of work affect how our services, commissioning or procurement activities are organised, provided, located and by whom?	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Could this piece of work affect the workforce or employment practices?	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Does the piece of work involve or have a negative impact on: <ul style="list-style-type: none"> • Eliminating unlawful discrimination, victimisation and harassment • Advancing quality of opportunity • Fostering good relations between protected and non-protected groups in either the workforce or community 	<input type="checkbox"/>	<input checked="" type="checkbox"/>

If you have answered no to the above and conclude that there will not be a detrimental impact on any equality group caused by the proposed policy/project/service change, please state how you have reached that conclusion below:

No detrimental impact identified on any projected characteristic group. Policy is a staff implementation policy.

If you have answered yes to any of the above, please now complete the 'STEP 2 Equality Impact Assessment' document

Accessible Information Standard	Yes	No
Please acknowledge you have considered the requirements of the Accessible Information Standard when communicating with staff and patients. https://www.england.nhs.uk/wp-content/uploads/2017/10/accessible-info-standard-overview-2017-18.pdf	<input checked="" type="checkbox"/>	<input type="checkbox"/>
If any of the above have not been implemented, please state the reason:		
Not applicable		

Governance, ownership and approval

Please state here who has approved the actions and outcomes of the screening		
Name	Job title	Date
Irene Walker	Head of Governance	September 2020

Publishing

This screening document will act as evidence that due regard to the Equality Act 2010 and the Public Sector Equality Duty (PSED) has been given.

Duties and Responsibilities

<p>Accountable Officer</p>	<p>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 usually carried out by the Executive Director of Nursing and Chief Operating Officer.</p>
<p>Line Managers</p>	<p>Line Managers have a responsibility to:</p> <ul style="list-style-type: none"> • Develop and support the implementation of the Policy and ensure the CCG meets national and local requirements
<p>All staff</p>	<p>All staff have a responsibility to:</p> <ul style="list-style-type: none"> • 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 NECS Information Governance service 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', obtain authorisation from main signatory. All staff must ensure there is a clear audit trail of authorisation and that written permission is obtained from main signatory, prior to correspondence being sent or circulated.