Title	SCCI1596 Secure Email Requirements Specification		
Document ID	SCCI1596 Amd 3/2016		
Sponsor	Dr. Simon Eccles	**Status**	Final
SRO	Cleveland Henry	**Version**	2.0
Author	Chris Parsons	**Version Date**	25/01/2017

SCCI1596 Secure Email Requirements Specification

Amendment History:

Version	Date	Amendment History
1.3	30/11/2015	Updated to reflect changes to central guidance
1.4	06/01/2016	Updated to remove the reference to CIO Council Offshoring Position
1.5	14/07/2016	Updated to reflect new Programme Director
1.6	30/09/2016	Updated customer need, IG references and hyperlinks.
1.7	14/10/2016	Updated interoperability statement
1.8	16/11/2016	Amended glossary to include technical terms
1.9	10/01/2017	Amendments made as per ISAS comments
2.0	25/01/2017	Included comments from SCCI forum

Approvals:

Name	Title / Responsibility	Date	Version
Dr Simon Eccles	Sponsor – NHSmail	26/01/2017	2.0
Cleveland Henry	SRO	26/01/2017	2.0

SCCI Standardisation Committee for Care Information

This information standard (SCCI1596) has been approved for publication by the Department of Health under section 250 of the Health and Social Care Act 2012.

Assurance that this information standard meets the requirements of the Act and is appropriate for the use specified in the specification document has been provided by the Standardisation Committee for Care Information (SCCI), a sub-group of the National Information Board.

This information standard comprises the following documents:

- Requirements Specification
- Change Specification
- Implementation Guidance.

An Information Standards Notice (SCCI1596 Amd 3/2016) has been issued as a notification of use and implementation timescales. Please read this alongside the documents for the standard.

The controlled versions of these documents can be found on the NHS Digital website. Any copies held outside of that area, in whatever format (e.g. paper, email attachment), are considered to have passed out of control and should be checked for currency and validity.

Date of publication: 15 March 2017

Glossary of Terms:

Term	Acronym	Definition
Clinical Authority To Release	CATR	An approval to release an IT system, service or process into live clinical environment.
Communications-Electronics Security Group	CESG	CESG is the UK government's national technical authority for information assurance (IA). It protects the UK by providing policy and assistance on the security of communications and electronic data, in partnership with industry and academia. CESG became part of the NCSC on 3 October 2016.
Communications Listed Advisor Scheme	CLAS	A former Government scheme to manage a list of Information Security/Assurance professionals who have been vetted, assessed and approved by CESG to advise the UK Government (and its key suppliers, such as defence contractors, System Integrators and the like). It has been replaced by the the Certified Cyber Security Consultancy CESG and CAS scheme.
Department of Health	DH	DH is the ministerial department of the United Kingdom government responsible for government policy on health and adult social care matters in England, along with a few elements of the same matters which are not otherwise devolved to the Scottish Government, Welsh Government or Northern Ireland Executive. It oversees the English National Health Service (NHS). The Department is led by the Secretary of State for Health with a Minister of State and four Parliamentary Under-Secretaries of State.
Digital Marketplace		The online platform that all public sector organisations can use to find and buy cloud-based services (e.g. web hosting or site analytics).
Domain Keys Identified Mail	DKIM	DKIM is an authentication mechanism to help protect both email receivers and email senders from forged and phishing email.
Domain-based Message Authentication, Reporting & Conformance	DMARC	Is an email authentication protocol.
eDiscovery		Electronic discovery (or e-discovery or eDiscovery) refers to discovery in civil litigation or government investigations which deals with the exchange of information in electronic format.
Enterprise Control	EC	A baseline control set control that applies to an enterprise rather than a specific system.
Health and care organisations		Any organisation, whether public, private or 3rd sector, delivering publicly funded health, public health and adult social care.
Health and Social Care Information Centre	HSCIC	Now known as NHS Digital. The national provider of information, data and IT systems for commissioners, analysts and clinicians in health and social care.
Information Commissioner's Office	ICO	The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

Term	Acronym	Definition
Information Governance Toolkit	IGT	The IG Toolkit is an online system which allows organisations to assess themselves or be assessed against Information Governance policies and standards.
Information Security Management System	ISMS	An information security management system (ISMS) is a set of policies concerned with information security management or IT related risks. The idioms arose primarily out of BS 7799. The governing principle behind an ISMS is that an organisation should design, implement and maintain a coherent set of policies, processes and systems to manage risks to its information assets, thus ensuring acceptable levels of information security risk.
International Organisation for Standardization	ISO	Developer of international standards for organisations, for example ISO 27001 Information Security Management Systems.
National Information Board	NIB	The role of the National Information Board is to oversee data and technology safely in to work for patients, service users, citizens and the professionals who serve them.
National Cyber Security Centre	NCSC	The National Cyber Security Centre (NCSC) is the UK's authority on cyber security.
NHS Digital		NHS Digital is the preferred name for HSCIC (above). NHS Digital is the national provider of information, data and IT systems for commissioners, analysts and clinicians in health and social care.
NHSmail		Secure email service recommended for health and care.
Risk Management and Accreditation Document Set	RMADS	Document set evidencing appropriate management of risks.
Safety Case		A safety case is a document produced by the operator of a facility which: Identifies the hazards and risks. Describes how the risks are controlled. Describes the safety management system in place to ensure the controls are effectively and consistently applied.
Standardisation Committee for Care Information	SCCI	The Committee oversees the development, assurance and approval of information standards, data collections and data extractions (ISCE) for use in health and care in England.
Sender Policy Framework	SPF	An SPF record is a type of Domain Name Service (DNS) record that identifies which mail servers are permitted to send email on behalf of the organisations domain. The purpose of an SPF record is to prevent spammers from sending messages with forged From addresses at an organisations domain.
Secure/Multipurpose Internet Mail Extensions	S/MIME	A protocol, for sending digitally signed and encrypted messages.
Transport Layer Security	TLS	Transport Layer Security (TLS) is a protocol that ensures privacy between communicating applications and their users on the Internet. When a server and client communicate, TLS ensures that no third party may eavesdrop or tamper with any message. TLS is the successor to the Secure Sockets

Term	Acronym	Definition
		Layer (SSL). For secure email, forced TLS means encrypt and fail if not possible, opportunistic TLS means encrypt if possible, send in the clear if not.
The United Kingdom Accreditation Service	UKAS	Is the sole national accreditation body recognised by the British government to assess the competence of organisations that provide certification, testing, inspection and calibration services.
World Wide Web Consortium	W3C	The World Wide Web Consortium (W3C) is an international community that develops open standards to ensure the long-term growth of the Web.

The standard uses RFC2119 definitions for MUST, SHOULD and MAY as given below:

Term	Definition
MUST	This word, or the terms "REQUIRED" or "SHALL", means that the definition is an absolute requirement of the specification.
MUST NOT	This phrase, or the phrase "SHALL NOT", means that the definition is an absolute prohibition of the specification.
SHOULD	This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
SHOULD NOT	This phrase, or the phrase "NOT RECOMMENDED", mean that there may exist valid reasons in particular circumstances when the particular behaviour is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label.
MAY	This word, or the adjective "OPTIONAL", means that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item.

Contents

1 Overview

1.1 Summary

Standard	
Standard Number	SCCI1596
Title	Secure Email
Description	This standard defines the minimum non-functional[1] requirements for a secure email service, covering the storage and transmission of email. This is the basic level for the storage and transmission of patient identifiable data by an email system. It includes: • The information security of the email service. • Transfer of sensitive information over insecure email. • Access from the Internet or mobile devices. • Exchange of information outside the boundaries of the secure standard. It excludes: • Security standards for document archives. • Specific technical solutions for communicating with insecure email services. • Email systems that are not intended to process official and or personal identifiable data. • Technical security controls that might be used to make a more secure email system, for example two factor authentication, digital signatures. Note: • Official information must always be managed in accordance with the published HM Government Security Classifications. Personal identifiable data must be managed in accordance with the Department of Health's published guidance on NHS Confidentiality Code of Practice.
Applies to	This information standard applies to all health and care organisations: • public, private and third sector organisations commissioned in delivering publicly funded health, public health and adult social care • commissioned Email service providers (any commissioned supplier providing email services within health and care) • commissioners of health and care within England.

[1] A functional requirement describes what a software system should do, while non-functional requirements place constraints on how the system will do so. This is elaborated at: http://stackoverflow.com/questions/16475979/what-is-functional-and-non-functional-requirement

Impacts upon	Implementation of this information standard and its revision impacts all IT service providers of email systems to the above providers and commissioners. IT service providers should work with their customers to determine necessary changes.
Release	
Release Number	Amd 3/2016
Title	Version 2.0
Description	This release introduces changes to a number of the requirements, following updates to Cabinet Office guidance. These relate to: • ISO 27001 updated to the 2013 version. • Removing of CESG guidance references – IS1/IS2, Business Impact Levels and the CLAS scheme. • Removing of ISB 1596 tailored Baseline Control Set. The controls are sufficiently detailed in BS ISO/IEC 27001:2013 and the requirement of independent baseline control set audit as part of BS ISO/IEC 27001: 2013 ensures a strong level of compliance verification. • Inclusion of additional Cabinet Office guidance - email security/authenticity controls (TLS, SPF, DKIM and DMARC). The service should support Domain Based Message Authentication and Reporting (DMARC) with supporting public Domain Name System (DNS) entries for Sender Policy Framework (SPF) and sign outgoing email in accordance with the Domain Keys Identified Mail (DKIM) standard. • Removal of the need to have a PSN code of connection. • Removal of the email router. Each service provider MUST enable forced TLS inbound and outbound for secure email delivery and opportunistic for all other emails. The release also allows for uplift of the current ISB 1596 Secure Email information standard to comply with the Health and Social Care Act 2012.
Implementation Start Date	Changes may be implemented with immediate effect.
Full Conformance Date	September 2017

1.2 Guidance

Ref no	Title	Version
1	Information: To Share Or Not To Share? The Information Governance Review (Caldicott 2)	
2	The Good Practice Guidelines for GP electronic patient records	4

Ref no	Title	Version
3	General Medical Council Good Medical Practice	2013
4	Government Interoperability Open Standards	Update 11 Sept 2015
5	National Data Guardian for Health and Care: Review of Data Security, Consent and Opt-Outs	June 2016

1.3 Related Standards

Reference	Title
SCCI0086	Information Governance Toolkit
SCCI0160	Clinical Risk Management: its Application in the Deployment and Use of Health IT Systems
SCCI0129	Clinical Risk Management: its Application in the Manufacture of Health IT Systems
BS ISO/IEC 27001:2013	Information technology -- Security techniques -- Information security management systems -- Requirements
BS ISO/IEC 27002:2013	Information technology. Security techniques. Code of practice for information security controls
Cabinet Office Guidance	https://www.gov.uk/guidance/securing-government-email
RFC5246 (TLS)	https://tools.ietf.org/html/rfc5246
RFC7208 (SPF)	https://tools.ietf.org/html/rfc7208
RFC6377 (DKIM)	https://tools.ietf.org/html/rfc6377
RFC7489 (DMARC)	https://tools.ietf.org/html/rfc7489

2 Introduction

2.1 Purpose

Emails sent from and to NHSmail accounts, or to other secure email systems, are protected by UK Government standards. This ensures that sensitive and confidential information is kept safe.

NHSmail meets the Secure Email Standard (SCCI1596). Any health and care organisation wishing to operate its own email systems securely and connect to other secure email services such as NHSmail must meet the requirements to the standard.

This standard establishes the minimum requirements for email systems in health, public health and adult social care. The intention is not to impose significant requirements on organisations but instead to establish the minimum acceptable level. Where appropriate organisations seeking accreditation to this standard will refer to health and care, Government and international standards (e.g. ISO/IEC 27001 – see related standards). In addition to achieving ISO 27001, it is the responsibility of the organisation procuring the email system to understand and accept any risks and issues associated with their email system and commissioned provider.

As well as defining basic requirements for any email service, the standard defines how email systems used for personal and sensitive data (e.g. patient identifiable data) should manage the information security of the email service.

Non-NHS organisations who are currently accredited to the government secure email standard are out of scope for this secure email standard.

2.2 Customer Need

Health and care email is now a rich source of patient/service user information. There is a clear need to ensure that it is held securely and used appropriately. With the increase in cyber-attacks and threats, keeping data secure is critical. The recent Caldicott review [5] on data security highlighted the need for simplified cyber security which is achievable and easy to understand – Paragraph 2.6.4 specifies (our bold text):

“The Review concludes that the organisations facing most risk are those with lower existing capabilities. Therefore the starting point in addressing cyber security must be simplified as far as possible to encourage full understanding, and be achievable within already stretched budgets.”

The Secure Email Standard is aligned to NIB Work Stream 4 which reinforces a need to ensure that “citizens’” health data is managed securely. The standard will ensure that health, public health and adult social care organisations have a recognisable baseline which they can conform to ensuring emails are transmitted securely.

3 Health and Care Organisations

Emails sent from and to NHSmail accounts, or to other secure email systems are protected to UK Government standards. This ensures that sensitive and confidential information is kept safe.

NHSmail meets the Secure Email information standard (SCCI1596). Any health and care organisation wishing to operate its own email systems securely and connect it to other secure email services such as NHSmail must meet the standard.

Organisations need to complete the service user element of the standard and configure their local system accordingly.

3.1 Overview

The current SCCI0086 Information Governance Toolkit (IGT) (as an already approved information standard and its future revision) provides the strategic assurance tool for use by all health and care service providers, commissioners, suppliers and business partners. It has a series of requirements that all health and care organisations including commissioners and suppliers must meet, with the information security requirements being particularly applicable. This standard describes how health and care organisations can comply with the IG Toolkit with respect to email services.

Organisations should seek guidance from their local Information Governance team on details of the exact requirements.

3.2 Requirements

The following table represents the Requirements for this standard:

Num	Description
Information Security	
1	Each Service Provider MUST have an independent IT Health Check (ITHC) / penetration test carried out (by a CHECK / Tigerscheme accredited or CREST member organisation) encompassing the email system and external network interfaces (including perimeter security / access control devices). Evidenced by a recent ITHC / penetration test report, with all identified risks mitigated, and any residual risks accepted.
2	Either party (Service Provider or commissioner) MUST notify the other immediately upon becoming aware of any breach of security, including an actual, potential or attempted breach of, or threat to, the security policy and/or the security of the services or the systems used to provide the services.
3	Health and care organisations MUST operate their email service to a level appropriate to the security risk assessment, with an ISO/IEC 27001:2013 compliant ISMS as a minimum.

4	Health and care organisations, whose email service processes patient identifiable or sensitive data, MUST ensure the ISMS relevant to the email service complies with relevant ISO/IEC 27001:2013 information security controls.
5	Health and care organisations MUST set policies and procedures for the use of secure email using mobile devices and ensure the email service enforces them.
Safety	
6	Health and care organisations SHOULD comply with the provisions of SCCI0160 Clinical Risk Management: its Application in the Deployment and Use of Health IT Systems.
7	Health and care organisations SHOULD set policies and procedures for staff who use the secure email service to ensure that they understand how to use it appropriately and safely.
Interoperability	
8	Health and care organisations MUST ensure there are appropriate policies in place for the use of email, including correspondence with insecure email systems such as those used by patients.

3.3 Conformance

Health and care organisations shall self-certify to the standard using the evidence listed below. If the organisation also runs its own internal email service it must also comply with the IT Service Provider requirements in section 4 below. Health and care organisations will be required to submit their evidence to NHS Digital for review, and a conformance statement will be made available to view on the NHS Digital website.

Information Security

- Evidence of a security risk assessment for the email service.
- A completed Information Governance Toolkit submission (at level 2 or 3).
- An auditable Information Security Management System (ISMS) relevant to the email service that conforms to ISO/IEC 27001:2013.
- Published policies and procedures for the use of secure email using mobile devices.
- Evidence provided by the email service provider that they have met this standard.

Clinical Safety

- Organisations should have a documented Clinical Risk management process as per SCCI0160 Clinical Risk Management: its Application in the Deployment and Use of Health IT Systems.

Interoperability

- Published policies for the use of email with insecure systems.

4 IT Service Providers

4.1 Overview

Organisations must ensure that they have adequate contractual terms agreed with their Service Providers safeguarding that the commissioned email service meets the needs of health and care, especially when it is used for the transmission of patient identifiable data. Email systems are not normally sector specific (i.e. just for health and care) so IT service providers will normally demonstrate this through adherence to cross-public sector, UK or international standards.

Note that any health and care organisation using an internally run email service is an IT service provider and must comply with this section. In addition to achieving ISO 27001, it is the responsibility of the organisation procuring the email system to understand and accept any risks and issues associated with their email system and commissioned provider.

4.2 Requirements

Num	Description
Information Security	
1	Each Service Provider MUST at all times maintain a secure service, even when the service is unavailable to users.
2	Each Service Provider MUST maintain an Information Security Management System (ISMS) that conforms to ISO/IEC 27001:2013, based on ISO/IEC 27002:2013 Information technology - Security techniques - Code of practice for information security controls. Conformance should be evidenced by appropriate certification by a United Kingdom Accreditation Service (UKAS)[2] accredited certification organisation.
3	The information security controls contained within the scope, on which each Service Provider's ISO/IEC 27001:2013 certification is based, MUST be relevant to the email service. Conformance should be evidenced by the applicable Statement of Applicability (SoA).
4	Each Service Provider MUST maintain a security policy which sets out the security measures to be implemented and maintained in accordance with ISO/IEC 27001:2013, ISO/IEC 27002:2013 and the Information Security Management System. The security policy MUST be reviewed and updated by the Service Provider at least annually, and MUST be endorsed by the Service Provider's senior management. If requested by NHS Digital, a copy MUST be made available.
5	Each Service Provider MUST have a suitably scoped independent IT Health Check / penetration test carried out (by a CHECK / Tiger scheme accredited or CREST member organisation) encompassing the email system and any external network interfaces (including perimeter security / access control devices).

[2] https://www.ukas.com/search-accredited-organisations/

	Conformance should be evidenced by an ITHC / penetration test report conducted within the last 12 months, with all identified findings remediated/mitigated, and any residual risks accepted.
6	Either party (Service Provider and commissioner of the email service) MUST notify the other immediately upon becoming aware of any breach of security, including an actual, potential or attempted breach of, or threat to, the security policy and/or the security of the services or the systems used to provide the services.
7	Each Service Provider MUST provide protection against malicious content for their services such as virus/malware checking when on-boarding data. The commissioner of the email service must ensure adequate policies and/or contractual agreements are in place to safe guard this.
8	The email service MUST provide anti-virus, anti-malware and anti-spam filtering, in addition to commodity content management such as attachment blocking, virus/spam filtering capabilities and data leakage prevention e.g. encrypt protectively marked email destined for the Internet. The service SHOULD also provide for the management of spoofed email and items that cannot be checked such as S/MIME encrypted or password protected attachments. The service should support Domain Based Message Authentication and Reporting (DMARC) with supporting public Domain Name System (DNS) entries for Sender Policy Framework (SPF) and sign outgoing email in accordance with the Domain Keys Identified Mail (DKIM) standard.
9	All patient identifiable and Government OFFICIAL SENSITIVE data MUST be maintained in accordance with the Information Commissioner's Office data protection guidance paying particular note to Principle 7 and the guidance on the use of cloud computing..
10	The Service Provider MUST provide tools to ensure that mobile devices are appropriately secured when accessing the email service. This should include: • Functions to allow/deny/quarantine by device type, organisation or groups of users. • Remove device, expire password, and wipe any data associated with the service. • Reporting functions/ capabilities. • Detect and block rooted (e.g. jail broken) devices.
11	Each Service Provider MUST provide eDiscovery tools to support the administration of the service, especially with respect to the Data Protection Act 1998 and Freedom of Information Act 2000.
Safety	
12	Service Providers SHOULD comply with the provisions of SCCI0129 Clinical Risk Management: its Application in the Manufacture of Health IT Systems.
Interoperability	
13	Each Service Provider SHOULD comply with the open standards principles.
14	Each service provider MUST enable inbound and outbound Transport Layer Security (TLS) version 1.2 or better for secure email transport between other secure email services.
15	TLS Ciphers should conform with current NCSC guidance.

4.3 Conformance

Service Provider conformance shall be evidenced through external accreditation. This evidence shall be inspected by the health and care organisation using the service.

Information Security

For services using personal or sensitive data, the following is required:

- An independently audited Information Security Management System (ISMS) relevant to the email service. This shall be evidenced by ISO/IEC 27001:2013 certification issued by a United Kingdom Accreditation Service (UKAS) accredited organisation. The information security controls contained within the scope, on which the ISO/IEC 27001:2013 certification is based, MUST be relevant to the email service.

- An ITHC / penetration test report conducted within the last 12 months, with all identified findings remediated / mitigated and any residual risks accepted.

Clinical Safety

- Clinical safety approval for the email service, as per SCCI0160 Clinical Risk Management: its Application in the Deployment and Use of Health IT Systems.

Interoperability

- Evidence of conformance to the open standards policy. There must be evidence demonstrating the system implemented supports standard web and email protocols such as https, IMAP, POP, SMTP, LDAP to name a few.

5 Technical Guidance

5.1 Implementation

Organisations should assess their current email service against the standard and determine if it conforms or not. If it does not then follow one of the following options:

- Bring the service up to the required level of conformance. This will normally require the Service Provider to employ an information security specialist to advise on ISO/IEC 27001:2013 and government accreditation.
- Procure a service that conforms to the standard. Most business grade email services will conform to ISO/IEC 27001:2013, whilst many consumer (typically free) email services do not. Business grade email services suitable for personal and sensitive data use are available on the Digital Marketplace and other frameworks available from the Crown Commercial Service.
- Having due regard to the standard, determine that conformance is not appropriate. Organisations will still be able to access the old NHS UK insecure email relay, but won't be able to send secure emails to people in the secure relay unless they use an in-house encryption overlay.

It should be noted that the security levels required for personal and sensitive data are for where the data is unencrypted in the email service. Suitably encrypted data (for example email attachments) is secure by default. The encryption method should conform to approved security standards and good practices.

5.2 Information Security

ISO/IEC 27001:2013 sets out the requirements for an Information Security Management System (ISMS). This is a structured means of managing information security risk within an organisation. It is used here as a common basis for information security.

5.3 Clinical Safety

Any IT system used for clinical purposes must follow the clinical safety information standards. An example hazard log is provided in Appendix 1.

5.4 Interoperability

Systems should conform to open standards for interoperability, normally promulgated by the W3C. Government open standards are published on data.gov.uk.

Systems should populate national directory services. Details of how to populate the NHSmail directory are available from feedback@nhs.net.

Systems can interoperate securely using:

- Government approved secure interoperability standards
- Secure TLS point to point connections.
- S/MIME or other email encryption.

Note that communication between NHS.uk systems should not be considered secure as the national email relay service is not currently accredited to the appropriate level of security. Communication between NHSmail (@nhs.net, *secure.nhs.uk) addresses and Government Secure Networks (GSI, GCF, GSE, GCSX, MoD, Police, and Criminal Justice) is secure.

Secure systems will necessarily need to communicate with other untrusted email systems, for example when emailing the private sector (e.g. lawyers), other parts of the public sector (e.g. school nurses) or patients. Patient data should never be sent electronically without encryption regardless if patient consent has been provided or not. Such data being sent to untrusted email services should use the email encryption service either provided by NHSmail or through a certified secure email system. Confidential personal information must only be shared and used in a lawful manner and objections to the disclosure or use of this information must be appropriately respected. There must be a legitimate reason to share the data.

6 User Guidance

This section provides pointers to relevant guidance in support of the standard. Health and care organisations should use this and other published guidance to develop policies and procedures for staff using the secure email service.

6.1 Emailing Patients

The Caldicott 2 review [1] noted the belief that emails should only be used to communicate with patients when consent has been given and risks of email usage are understood and accepted. The review report stated:

> "The Review Panel concludes that personal confidential data can be shared with individuals via email when the individual has explicitly consented and they have been informed of any potential risk."

Health and care organisations should develop guidelines for health and care professionals to support and encourage the use of email with patients. The Good Practice Guidelines (paragraph 11.6 Using the Internet for Consulting) for GP electronic patient records describe the use of email for patient consultations.

6.2 Secure Communications

NHS information security guidelines require that patient identifiable or sensitive data is handled appropriately. For routine communication this should be within a secure email service, or sent in a secure manner, for example encrypted attachments that comply with the NHS encryption requirements.

Caldicott 2 established a 7th principle:

> "The duty to share information can be as important as the duty to protect patient confidentiality."

Security and this standard should be an enabler for good quality care. The onus is to provide appropriate systems and so share information, not inhibit it.

6.3 Professional Record-keeping

In the Good Medical Practice (2013), the General Medical Council (GMC) states that

> "19. Documents you make (including clinical records) to formally record your work must be clear, accurate and legible. You should make records at the same time as the events you are recording or as soon as possible afterwards.
>
> 20. You must keep records that contain personal information about patients, colleagues or others securely, and in line with any data protection requirements."

Although ephemeral in nature, emails can form part of the clinical record. Good practice is to ensure that emails are copied into the patient's medical record. See the Medical Protection Society Good Records advice for further information.

6.4 Data Protection and Freedom of Information

Information stored in an email service is subject to data protection and freedom of information requests. All health and care professionals must be aware of this obligation and support such requests.

6.5 GP Practice Staff

The Good Practice Guidelines for GP electronic patient records describe the use of email in practice, noting that.

> "Unless practices have the technical expertise to set up and maintain a local mail server, and ensure that it is secure within the practice network boundaries, the recommended approach is to use NHSmail for this purpose. NHSmail is available in Scotland and England."

Appendix 1 – Example Hazard Log

Overview

The example hazard log has been derived from secure email clinical risk assurance undertaken by NHS Digital. This is not an exhaustive list and should not be used as such. A hazard assessment should be undertaken in accordance with the clinical risk management standards and implementation guidance.

Hazard Log

Email is a communication system. The two biggest areas that could impact care are:

- Information is incorrectly communicated or delayed, for example an email becomes corrupt, meaning that care is compromised.
- Information is not communicated, for example because the service was unavailable, meaning that care is compromised.

Any hazard assessment will require the need for mitigating actions by taking the purpose of email in the context of the business process. Beyond this there are other hazards that derive from these two areas. These are given below.

Area	Hazard Name	Description	Effect
Email	Email notifications fail to arrive	Failure to receive email notification of error message.	The sender does not receive notification of email failure. Potential delay in treatment by way of failure to receive / send email.
Email	Email eDiscovery	Lack of traceability for investigations into incidents where recipients claim one or more emails never arrived.	The email itself is disputed, which may have medico-legal implications in cases where the email is evidence.
Attachment	File attachment issues	File attachments exceed mail system specified limits. File attachments exceed mail system specified attachment quantity limits. Incorrect file formats used when attached to email.	Delay to email transmission. Potential system error resulting from oversize files attachments. Failure to transmit / receive email successfully including potential loss of data. Potential system error resulting from large quantities of file attachments.
Attachment	File Attachments -	File attachment contains corrupt data	Inadequate validation on corrupt data files or email content results

Area	Hazard Name	Description	Effect
	Corrupt file attachments	undetected at source.	in loss of data or potential corruption of recipient systems.
Attachment	File Attachments - files contain software virus	File attachment or email content contains virus.	Potential partial or complete system failure. Loss of data at source or recipient systems. Potential loss of service.
IT operations	IT Operations - Inadequate Backup / Archive Process / System	Loss or inadequate backup and / or archiving processes/systems.	Failure to run backup process. Potential loss of service resulting from erroneous recovery points. Lack of recovery position leads to loss of data.
IT operations	IT Operations - Inadequate Failover procedures	Insufficient IT operational procedures covering failover and recovery positions.	System does not failover into a known stable state. Potential loss of service and data resultant.
IT operations	IT Operations - Inadequate Rollback process	Inadequate process / system configuration to allow secure email solution to recover to a known stable system state.	At the point of error the email system cannot rollback to baseline configuration leading to potential unstable state, loss of service/data.
IT operations	IT Operations - Insufficient Disk Space	Lack of hardware storage used at any point within the secure email system where temporary or permanent data is required.	Email system performance issues due to inefficient storage loads.
IT operations	Document Archive	Chosen mail solution used as a document archive at Local Level.	Potential loss of service and / or data due to inadequate storage facilities.
IT operations	IT Operations - Insufficient Security compliance	Security procedures and / or configuration are not fit for purpose of email system proposed usage.	Potential security breaches leading to unauthorised access to personal identifiable data, and commercially sensitive information. System is vulnerable to security attacks variable in nature - causing system failure, loss of data, and other business critical failures.
IT operations	IT Operations - Email Receipt notification fails to arrive	Secure mail system fails to provide receipt during email transmission process.	Failure to receive receipt notifications could lead to resubmissions throughout the email transmission process. This would in turn increase messaging volumes and increase the potential for delays in system performance.
IT operations	IT Operations - Delays in end to end processing of email	Email system and / or performance issues lead to significant delays in transmission at any point within the email pathway to	Potential loss / delay of service. Potential loss of data.

Area	Hazard Name	Description	Effect
		recipient.	
Deployment	Network Issues on deployment	Deployment of secure email results in network failures / issues at local or national levels, local network, or LAN performance and / or availability issues.	Network availability restrictions result in limited business functionality. Potential issues leading to the mail solution impacting user base day to day system performance and availability.
Deployment	Deployment of email system - Leading to Firewall / Routing issues	Deployment and configuration of firewall / routing infrastructure fails to complete successfully.	Restriction in messaging routing. Complete loss of service due to incorrect configuration of firewalls.
Deployment	Anti-Spam filter stops valid emails	The anti-virus anti-spam filter stops valid emails (a false positive) resulting in the email not being delivered. This include: • Anti-malware software incorrectly blocks an email or removes an attachment • Anti-spam software incorrectly files an incoming email (that is free of malware) in junk mail or spam folder.	The sender does not receive notification of email failure. Potential delay in treatment by way of failure to receive / send email.
Deployment	Deployment of email system - Leading to 'Clash' of Software Tools	Deployment of email system leads to conflicts with existing system software.	Potential performance issues with conflicting systems.
Desktop/Client	Desktop / Client - Badly Configured	Inadequate / poorly configured desktop and client infrastructure.	Inability to standardise and deploy email system. Increased volumes of helpdesk requests on non-standard hardware. Inability to install email system on unsupported hardware. Inadequate system performance leading to complete system failure. Potential loss of existing business processes.
	Desktop / Client - "Old"	Target desktop and client systems are outside the baseline limitations and recommendations for email usage. Note this can include old email services not being compatible with new browsers.	

Area	Hazard Name	Description	Effect
Desktop/Client	Desktop / Client - Unsuitable Windows versions	Existing operating system is outside the baseline supported configuration.	Inability to install email system on target hardware. Poor configuration leading to operational issues and increased helpdesk calls. Potential inefficient email service levels.
Desktop/Client	Desktop / Client – Setup / Migration wrong	Email service setup and migration fails to complete successfully on target system.	Potential performance issues with poorly configured systems. Loss of data due to incorrectly setup storage and archiving facilities.
Desktop/Client	Desktop / Client - Local Connectivity Issues	Local System issues lead to inability to connect to the email service	Potential performance issues leading to complete loss of service.
Desktop/Client	Desktop / Client - Too many windows open	Large number of local desktop sessions exceeds 'normal' expected operational levels.	Email system connectivity issues and performance issues due to increases processing constraints.
Misuse	Misuse - IG / Unauthorised Access	Email system used inappropriately, contravening IG security controls / guides.	Potential breach in IG policies/controls leads to source email information compromise. Breaches in security protocol and local / national policies for mail usage. Potential to misuse system not having appropriate access/training leading to severe email issues.
		Email system operation by end user who does not have access or approval to use the system.	
Misuse	Misuse – Consent	Inappropriate use of mail system without expressed consent of data source or system authorities.	Potential breaches of information sharing and overall system usage.
Misuse	Misuse – Hacking	Email system is targeted by external or internal hacking or attempts to connect in a manner not permitted by existing IG/security controls.	Inappropriate access to email system data, personal identifiable or business critical information. Critical misuse implications if undetected - complete loss of service, data tampering, etc.
Misuse	Misuse - Internal Fraud	Existing authorised user attempts to fraudulently operate email system	Internal Fraud covers various targets for misuse and may lead to inappropriate email usage, authorisation messages, and potential access to business or personally critical systems.
Misuse	Misuse – Browsing	Inappropriate use of email system resulting in browsing of group/personal mail accounts.	Access to information outside of normal controls for end users. Potential conflicts of business operation due to inappropriate data access, security breaches, etc.

Area	Hazard Name	Description	Effect
Migration	Data Migration	Errors / poor quality migration of legacy or existing email data.	Data Migration of legacy or email records
Functionality	New Functionality	Additional features of new email system / New functionality introduce issues with current service and / or existing functionality provided.	Potential loss / delay of service. Potential loss of data.
Functionality	Search	Poor search capability results in inability to find relevant email.	User unable to use information.
Training	Inadequate Training	Poor quality training on the new system leads to inappropriate email use.	Potential data loss. Potential inappropriate email usage based on 'not enough' or ineffective training.
Assurance/ Testing	Limited Test Assurance	Test strategy and scope does not fully assure the release of the new system	Potential loss / delay of service. Potential loss of data.
		Inadequate regression test assurance of existing / unchanged functionality.	
		Insufficient testing timeframe.	