Title	SCCI1596 Secure Email Change 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 Change Specification

Amendment History:

Version	Date	Amendment History
0.1	30/09/2016	Initial draft
0.2	03/10/2016	Updated branding
0.3	14/10/2016	Updated Glossary
0.4	15/11/2016	Removed duplicate link to Cabinet Office Guidelines
1.0	24/11/2016	Updated implementation completion date to April 2018
1.1	09/01/2017	Amendments made as per the comments from ISAS review
1.2	25/01/2017	Updated exclusion as per SCCI comments.
2.0	15/03/2017	Publication copy

Approvals:

Name	Title / Responsibility	Date	Version
Dr Simon Eccles	Sponsor – NHSmail 2	26/01/2017	1.2
Cleveland Henry	SRO	26/01/2017	1.2

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
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.
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.
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.
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

Term	Acronym	Definition
		coherent set of policies, processes and systems to manage risks to its information assets, thus ensuring acceptable levels of information security risk.
Information Standards Notice	ISN	ISNs are published by SCCI to announce new or changes to information standards published under section 250 of the Health and Social Care Act 2012.
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.
NHS Digital		NHS Digital is the preferred name for the Health and Social Care Information Centre (HSCIC). NHS Digital is the national provider of information, data and IT systems for commissioners, analysts and clinicians in health and social care.
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 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.

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 Supporting Documents

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

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 Change Specification

2.1 Purpose of the Standard

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 it to other secure email services such as NHSmail must meet the requirements to the standard.

This standard established 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). It is the responsibility of the organisation procuring the email system to understand and accept any risks 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 New Items, updates and removals

The changes are minor and maintain the core value of the original ISB 1596 Secure Email standard. The revisions include additions to the minimum security for emails as per Cabinet Office guidance as well as the removal of independent baseline controls due to updates to the ISO 27001 standard in 2013.

The details of the changes are:

- 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.

- Removing of the need to have a PSN code of connection.
- Removing of the email router. Each service provider MUST enable forced TLS inbound and outbound for secure email delivery and opportunistic for all other emails.

