NHS Digital

DCB1596 Amd 75/2019

Secure Email
Version 2.3
Change Specification

Published 8 January 2020

Information and technology
for better health and care

Data Coordination Board

This information standard (DCB1596) has been approved for publication by the Department of Health and Social Care 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 Data Coordination Board (DCB), a sub-group of the Digital Delivery Board.

This information standard comprises the following documents:

- Change Specification
- Requirements Specification
- Implementation Guidance.

An Information Standards Notice (DCB1596 Amd 75/2019) 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: 9 January 2020

Contents

Overview

Summary

Standard	
DCB Unique Identifier	DCB1596 Amd 75/2019
Name	Secure Email Version 2.3
Description	This standard defines the minimum non-functional [1] requirement 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 and Social Care'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 (Children Social Care falls under the remit of the Department of Education. • Commissioned Email service providers (any commissioned supplier providing email services within health and care) • Commissioners of health and care within England.
Release	
Release Number	Amd 75/2019
Title	Version 2.3
Description	This release, Version 2.3, introduces a change removing the requirement for a local organisation to implement a secure domain (.secure.nhs.uk) in order to meet the standard.
Implementation Completion Date	31 March 2020

Supporting Products

Ref no	Title	Version
1	Information: To Share Or Not To Share? The Information Governance Review (Caldicott 2)	1
2	The Good Practice Guidelines for GP electronic patient records	4
3	General Medical Council Good Medical Practice	2014
4	Government Open Standards Principles	Update 5 April 2018
5	National Data Guardian for Health and Care: Review of Data Security, Consent and Opt-Outs	June 2016
6	Sharing sensitive information guidance	

Related Standards

Reference	Title
DCB0086	Data Security and Protection Toolkit
DCB0160	Clinical Risk Management: its Application in the Deployment and Use of Health IT Systems
DCB0129	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 and RFC 8446 (TLS)	https://tools.ietf.org/html/rfc5246 https://tools.ietf.org/html/rfc8446
RFC7208 (SPF)	https://tools.ietf.org/html/rfc7208
RFC6377 (DKIM)	https://tools.ietf.org/html/rfc6377
RFC7489 (DMARC)	https://tools.ietf.org/html/rfc7489
RFC8640 (TLS-RPT)	https://tools.ietf.org/html/rfc8460
RFC8461 (MTA-STS)	https://tools.ietf.org/html/rfc8461
Health and Social Care Guidance	NHS and social care data: offshoring and the use of public cloud services

Change Specification

Purpose of the Standard

This standard establishes the minimum requirements for email systems in health, public health and 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 (DSPT), Government (Mail Check and government accreditation) and international standards (e.g. ISO/IEC 27001 where applicable). In addition to achieving compliance, 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 which are currently accredited to the government secure email standard are out of scope for this secure email standard.

New Items, updates and removals

Version 2.3 introduces a minor change to the standard based on local organisation feedback and the operational difficulty in its implementation.

Feedback has been provided directly about the challenges of implementing a secure domain and the impacts of managing this requirement.

The update will allow organisations to meet the standard without mandating the implementation of a secure domain (secure.nhs.uk or thirdparty.nhs.uk). The primary aim of this change is to reduce the burden on organisations meeting the standard other than joining NHSmail and respond to end user organisation feedback and escalations.

All associated technical conformance requirements still apply dependant on the accreditation route. In addition, all organisations are still required to meet and provide relevant evidence before accreditation to the standard.

The current accreditation website will be used to provide evidence of those organisations that have accredited and should be used to signpost for evidence of accreditation.

NHS Digital will look to publish a text file that lists all the domains that have met the secure email standard enabling local organisations to programmatically apply their own mail transport rules without having to check the website.

Guidance for nhs.uk domains will be updated to advise senders they must first check the accreditation website for the secure email status of a nhs.uk domain and the NCSC mail check service (or other email domain status sites for non nhs.uk domains).

All the associated published guidance on sharing sensitive information [6] has been updated to reflect the removal of secure.nhs.uk as a trusted domain.

It is the responsibility of the local organisation in line with local IG policy to ensure local email is only sent to accredited email services or to otherwise ensure email is encrypted.