DCB1596 Amd 5/2019

Secure Email
Version 2.2
Change Specification

Published 8 April 2019

Information and technology
for better health and care

Copyright © 2019 NHS Digital

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 5/2019) 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: 8 April 2019.

© NHS Digital 2019

Glossary of Terms:

Term	Acronym	Definition
Department of Health and Social Care	DHSC	DHSC is the ministerial department of the United Kingdom government responsible for government policy on health and 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.
Data Security and Protection Toolkit	DSPT	The Data Security and Protection Toolkit (DSPT) is an online self-assessment tool for data security which allows organisations to assess themselves against Information Governance policies and standards.
Enterprise Control	EC	A baseline control set control that applies to an enterprise rather than a specific system.
Health and care organisations	H&SC	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 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.
NHS Digital		NHS Digital is the preferred name for HSCIC (above). NHS Digital is the national provider of information, data

© NHS Digital 2019

Term	Acronym	Definition
		and IT systems for commissioners, analysts and clinicians in health and social care.
NHSmail		Secure email service recommended for health and care.
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 organisation's domain. The purpose of an SPF record is to prevent spammers from sending messages with forged From addresses at an organisation's domain.
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

© NHS Digital 2019

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", mean 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.

© NHS Digital 2019

Contents

1. Overview 7

1.1 Summary 7
1.2 Supporting Products 8
1.3 Related Standards 8

2. Change Specification 9

2.1 Purpose of the Standard 9
2.2 New Items, updates and removals 9

© NHS Digital 2019

1. Overview

1.1 Summary

Standard	
DCB Unique Identifier	DCB1596 Amd 5/2019
Name	Secure Email Version 2.2
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 for 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 5/2019
Title	Version 2.2
Description	This release, Version 2.2, introduces a change which is intended to reduce the costs of implementation and align to central government changes to secure email. With the adoption of the Data Security Protection Toolkit (DSPT) Organisations may now use either the DSPT or ISO 27001 to achieve accreditation.
Implementation Completion Date	31 March 2020

© NHS Digital 2019

1.2 Supporting Products

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
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
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: off-shoring and the use of public cloud services

© NHS Digital 2019

2. Change Specification

2.1 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 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 DCB0086 Data Security Protection Toolkit (DSPT - 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 comply with the assertions and mandatory evidence items detailed in the standard. This standard describes how health and care organisations can comply with the DSP Toolkit with respect to email services.

This release, Version 2.2, introduces minor changes which are intended to reduce the costs of implementation. The changes are:

- Following the introduction of the Data Security and Protection Toolkit to help reduce burden and cost, Health and Social Care Organisations may now use their DSPT submission instead of ISO 27001:2013 certification. Additional information on DSPT is available at https://www.dsptoolkit.nhs.uk/.
- The standard has also been updated to clarify how risks identified on the IT Health Check must be managed and reflects the updated guidance issued by UK Government on anti-spoofing as detailed at https://www.gov.uk/guidance/securing-government-email.
- For transparency email providers are required to state on their conformance statement in which Country/ Countries data will be hosted.

© NHS Digital 2019