NHS Digital

DCB1596 Amd 75/2019

Secure Email Version 2.3 Implementation Guidance

Published 9 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 6/2019) 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

1. Overview

1.1. Glossary of Terms

Term	Acronym	Definition
A and PTR Record	A & PTR	An Address (A) Record is a type of DNS record used to control the location of a resource on the Internet. A Pointer (PTR) record resolves an IP address to a fully qualified domain name (FQDN) as an opposite to what A record does. PTR records are also called Reverse DNS records
Clinical Authority To Release	CATR	An approval to release an IT system, service or process into live clinical environment.
Clinical Safety Officer	CSO	A person within a manufacturer or health and care organisation responsible for ensuring the safety of a health or care IT System, in that organisation, through the application of clinical risk management.
Data Coordination Board	DCB	Responsible for publishing standards under section 250 of the Health and Social Care Act 2012. DCB is a sub-group of the Digital Delivery Board (DDB).
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.

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.
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 and Conformance	DMARC	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.
Health and social care organisations		Any organisation, whether public, private or 3rd sector, delivering publicly funded health, public health and adult 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.

Term	Acronym	Definition
SMTP MTA Strict Transport Security (MTA-STS)	MTA-STS	MTA-STS is a mechanism enabling mail service providers to declare their ability to receive Transport Layer Security (TLS) secure SMTP connections and to specify whether sending email servers should refuse to deliver to email systems that do not offer TLS with a trusted server certificate.
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		NHSmail is our secure email service approved by the Department of Health and Social Care for sharing patient identifiable and sensitive information. NHSmail, messaging, and sharing can be accessed by any Organisation commissioned to deliver NHS healthcare or related activities.
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; and describes the safety management system in place to ensure the controls are effectively and consistently applied.
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.
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.
Simple Mail Transfer Protocol Transport Layer Security	TLS-RPT	A standard that enables reporting of TLS connectivity problems experienced by applications that send email.

Term	Acronym	Definition
The United Kingdom Accreditation Service	UKAS	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.

1.2. Supporting Documents

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	

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

2. Introduction

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 social care (DSPT), Government (Mail Check and government accreditation) and international standards (e.g. ISO/IEC 27001:2013 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.

3. Purpose

The purpose of this document is to provide guidance to health and care organisations seeking to self-accredit to the DCB1596 Secure Email Standard.

This implementation guidance assists in getting the standard in and working.

An ‘email service’ describes any system sending emails on behalf of an organisation. This includes:

- Providing users with mailbox access.
- Internal relays email relays and gateways.
- Email filtering services.
- Third party applications or services that send email on behalf of the organisation, like transactional email services.

4. Implementation approach

The implementation of DCB1596 Secure Email standard is managed by NHS Digital with sponsorship from the DHSC. The principal approach is to provide support for health and care organisations requiring accreditation of their email solution to the standard. NHS Digital is providing a light-touch approach as the accreditation evidence process and submission is the responsibility of each health and care organisation.

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 email Service Provider to employ an information security specialist to advise on ISO/IEC 27001:2013 or the DSPT.

- Procure a service that conforms to the standard. Most cloud 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.

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. Data encrypted to agreed good practice standards is secure by default.

Any issues regarding the standard itself or change requests should be sent in to the NHSmail Programme Team via feedback@nhs.net.

5. Implementation

5.1. Encryption

Follow these steps to encrypt email services:

1. Use Opportunistic TLS version 1.2 or later and preferred cryptographic profiles for secure email transport between email systems.
2. Follow NCSC guidance on TLS to ensure you are following the latest guidance on TLS use. If you operate an internet-facing email service you must buy and manage appropriate TLS certificates from the Digital Marketplace.

The National Cyber Security Centre Mail Check service can be used to help setup and maintain good TLS configurations.

5.2. Anti-spoofing

To prevent email spoofing, you must put technical and business policies in place to check inbound and outbound email using DMARC.

1. Implement DMARC by:
2. Publishing a DMARC record starting at p=quarantine rising to p=reject during implementation and enabling inbound DMARC checking on your email service. Implementation to be completed within 3 months of accreditation.
3. Implement SPF by publishing public DNS records for SPF, including all systems that send email starting at soft fail (~all) moving to fail (-all). Implementation to be completed within 3 months of accreditation.
4. Implement DKIM by:
5. Publishing DKIM selector and policy records in line with NCSC guidance.
6. Signing outgoing email in accordance with the DKIM standard.
7. Have matching forward and reverse (A and PTR) DNS records for the sending host.
8. Implement MTA-STS and TLS-RPT if your email service supports this.

6. Conformance Evidence

6.1. Health and Care Organisations

6.2.1 Overview

The organisation or commissioner (of the email system) is responsible for providing evidence demonstrating the security of the email system regardless whether the email system is procured via an IT Service provider or is an in-house email system.

This evidence must be submitted to NHS Digital via feedback@nhs.net for review. Once approved an assurance certificate will be issued accrediting the email system for a maximum 12-month period after which it must be renewed.

Health and care organisations shall self-certify to the standard using the evidence listed below.

6.2.2 Information Security

Evidence is required of a security risk assessment being conducted for the email service. This can be:

- Evidence of a security risk assessment for the email service.
- A completed DSPT with all assertions and mandatory evidence items filled in.
- An auditable Information Security Management System (ISMS) relevant to the email service that conforms to ISO/IEC 27001:2013. (Evidence of this being in place may be supplied directly to NHS Digital by an ICT Service Provider, e.g. Microsoft).
- 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.

6.2.3 Risk Assessment

Health and social care organisations require evidence demonstrating completed security risk assessment.

6.2.4 Clinical Safety

Provide evidence of clinical safety approval for the email service, as per DCB0160: Clinical Risk Management: its Application in the Deployment and Use of Health IT Systems, including the acceptance of any associated residual risks by a suitable CSO.

6.2.5 Supporting Published Policies

Health and social care organisations must have published policies demonstrating email usage, including procedures for transmission to non-secure email services.

Evidence of policies and procedures for email usage on mobile devices is required. The policies must be published and be readily available for staff to access.

6.2.6 Mail Hygiene and Anti spoofing

Evidence is required to confirm the necessary controls are in place. This can be:

- Confirmation that anti-virus and anti-malware services are running on the service.
- The NCSC Mail Check service confirms that TLS, DKIM, DMARC and SPF are correctly configured. Initial policies set to quarantine with blocking implemented by the agreed timeline.
- Current status and intentions on MTA-STS as well as TLS-RPT.

6.3 Commissioned IT Service Providers

6.3.1 Overview

Commissioners/health and care organisations need to ensure adequate contractual terms are agreed with IT service providers ensuring that the email service meets the needs of health and care, especially when it is used for the transmission of patient identifiable data.

6.3.2 Information Security

The IT Service Provider must provide evidence confirming the ISMS encompassing the email service conforms to either DSPT completion for H&SC Organisations or ISO/IEC 27001:2013 for all other providers. This should be in the form of ISO27001:2013 certification by a UKAS accredited certification organisation, based on a suitably scoped Statement of Applicability relevant to the email service.

DSPT accreditations will be verified on the DSPT website.

6.3.3 Information Security

Evidence is required of a security risk assessment being conducted for the email service. This can be one of:

- A completed DSPT with all assertions and mandatory evidence items filled in.
- Evidence demonstrating the email service conforming to BS ISO/IEC 27001:2013.
- 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. It is noted that some internationally operated public cloud services may be accredited by another country. If so, it must be from a member of the International Accreditation Forum.
- An IT Health Check (ITHC) / penetration test report conducted within the last 12 months, with all identified findings remediated / mitigated, and any residual risks accepted.

6.3.4 Clinical Safety

Provide a Safety Case which must be submitted to NHS Digital and signed off with a CATR with conformance to DCB0129: Clinical Risk Management: its Application in the Manufacture of Health IT Systems

6.3.5 Supporting Published Policies

Health and care organisations must have published policies covering email usage including procedures for transmission to non-secure email services.

Evidence of policies and procedures for email usage from mobile devices is required. The policies must be published and endorsed by senior management.

6.3.6 Interoperability

Interoperability evidence is required to support conformance, 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:

- The Government Secure Networks.
- Secure TLS point to point connections.
- S/MIME or other email encryption.

6.3.7 Offshoring

Data must only be hosted in locations detailed in the NHS and Social Care cloud hosting and off-shoring Policy. As part of the conformance template suppliers are required to declare where personal/ sensitive data will be hosted.

6.4 Submission Process

Each organisation wishing to obtain accreditation to the standard must complete the relevant DCB1596 Conformance Assessment template (available on the NHS Digital website), with all required documentary evidence embedded in the evidence section. This should be forwarded to feedback@nhs.net for review by NHS Digital.

On satisfactory completion of the review process (approximately 10 business days depending on availability of appropriate NHS Digital resources) the agreed DCB1596 Conformance Assessment will be published on the NHSmail website.

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 DCB standards and implementation guidance.

Hazard Log

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 - Corrupt file attachments	File attachment contains corrupt data undetected at source.	Inadequate validation on corrupt data files or email content results in loss of data or potential corruption of recipient systems.
Attachment	File Attachments - files contain software	File attachment or email content contains virus.	Potential partial or complete system failure. Loss of data at source or recipient systems.

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
	virus		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.

Area	Hazard Name	Description	Effect
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 recipient.	Potential loss / delay of service. Potential loss of data.
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.

Area	Hazard Name	Description	Effect
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.

Area	Hazard Name	Description	Effect
Misuse	Misuse – Consent	Email system operation by end user who does not have access or approval to use the system.	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.
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.

Area	Hazard Name	Description	Effect
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.	