DCB1596 Conformance Assessment:

Google Cloud
Date: 27th July 2022
ICT Service Provider: Google Cloud EMEA Limited
Date of ICT Service Provider conformance: 30th July 2022

Secure Email Domains that will be used by this email service:

Purpose

This document provides the results of a conformance assessment undertaken by NHS Digital to assist health and care organisations who wish to self-accredit their services to DCB1596 Secure Email. This typically means that this organisation operates its own in-house email service.

Part of this document provides the results of a self-conformance assessment undertaken by Google Cloud covering the Health and Care elements of the DCB1596 Secure Email Standard. The ICT Service Provider section covers service controls.

Each organisation must make its own decisions with respect to the standard. The assessment is for a single point in time and does not give secure email connectivity between email systems. This requires connectivity with a secure email gateway or by using secure configuration settings.

Guidance Notes

The conformance statement issued is based on the Google Cloud Service assertions, supported by evidence.

The first section of this conformance statement only requires the dates at which each policy related requirement was achieved / published (for example, within the last 6 months) in agreement with their senior management. For the ICT Service Provider section, we require evidence that each requirement is met.

Elements of interest: That clear risk reports are presented, highlighting the residual risks that have been accepted and signed off by senior clinical safety and ICT members of staff in an organisation.

NHS Digital confirms a level of conformance was achieved, has authorised the creation of the email domain and that the evidence presented meets the requirements of the standard, but in no way warranties local compliance. This applies to email usage only and NHS Digital reserves the right to audit any information submitted.

ICT Service Provider

#	Requirement	Statement of Conformance
Information Security		
1	The Service Provider MUST at all times maintain a secure service, even when the service is unavailable to users.	**MET** Google's customers and regulators expect independent verification of our security, privacy, and compliance controls. In order to provide this, we undergo several independent third-party audits on a regular basis. For each one, an independent auditor examines our data centers, infrastructure, and operations. Regular audits are conducted to certify our compliance with the auditing standards ISO 27001, ISO 27017, ISO 27018, SOC 2 and SOC 3 Google Workspace (formerly GSuite) has been assessed as meeting the NCSC SaaS security principles: https://www.ncsc.gov.uk/collection/saas-security?curPage=/collection/saas-security/product-evaluations/g-suite
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 or the Data Security and Protection Toolkit (DSPT) in the case of health and social care organisations. ISO/IEC 27001: 2013 conformance may be evidenced by appropriate certification by a United Kingdom Accreditation Service (UKAS[1]) accredited certification organisation, based on a suitably scoped Statement of Applicability relevant to the email service. Internationally operated services may provide certification from a member of the International Accreditation Forum. DSPT submissions will be verified on the DSPT website.	**MET** Google Workspace (formerly GSuite) is certified as ISO 27001 compliant. Electronic copies of the latest certificates can be viewed at: https://cloud.google.com/security/compliance/iso-27001/ Google LLC (ODS Code: 8JE14) has completed registration with the Data Security and Protection Toolkit (DSPT)

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

3	If applicable, the information security controls contained within the scope, on which the Service Provider's ISO/IEC 27001:2013 certification or DSPT return is based, MUST be relevant to the email service. Conformance should be evidenced by the applicable Statement of Applicability (SoA).	**MET** The Google Workspace email service (Gmail) is entirely within the scope of the Google Workspace ISO 27001 compliance certificate available from https://cloud.google.com/security/compliance/iso-27001/ NHS Digital has verified that the full SoA covers the email service.
4	The Service Provider MUST maintain an Information Security Policy, as part of its ISMS (conforming to ISO/IEC 27001:2013, ISO/IEC 27002:2013) which sets out the security aims and objectives, as well as security measures to be implemented and maintained. The security policy MUST be regularly reviewed and updated by the Service Provider and MUST be endorsed by the Service Provider's senior management. A copy should be supplied as evidence.	**MET** Google Cloud Platform, our Common Infrastructure, Google Workspace, and Chrome (Chrome Services, Chrome Sync and Cloud Print only) are certified as ISO 27001 compliant. Google regularly reviews and updates where required our security policies with endorsement/sign off from Google senior management team. NHS Digital has as part of the accreditation process been provided with a copy of our Security and Compliance Whitepaper which provides further detail on our security measures.
5	Each Service Provider MUST have a suitably scoped independent IT Health Check (ITHC) / 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). 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 by the Senior Information Risk Owner. All risks are expected to be remediated unless there are exceptional reasons not to do so or in the view of NHS Digital is sufficiently mitigated.	**PARTIALLY MET** Google runs regular penetration tests against Google Workspace and our wider services, including FedRAMP. *It is the responsibility of each Organisation to perform ITHC against their own configuration, to ensure that your environment has been configured appropriately, and that remediation of findings is carried out and any residual risk is accepted by responsible Officer(s)* Organisations are **not** obliged to contact Google before undertaking penetration testing, provided the tests comply with the Acceptable Use Policy and Terms of Service. Tests should only be conducted against the Organisation's own instance of Gmail. Any vulnerabilities found can be reported to the Vulnerability Reward

		Program.
6	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, for example, encrypt protectively marked email destined for the internet. The service MUST 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 MUST support Domain Based Message Authentication and Reporting (DMARC) with supporting public Domain Name System (DNS) entries for Sender Policy Framework (SPF) set to quarantine with an agreed timeline to implement a blocking policy **no later than 3 months after accreditation**. All outgoing email MUST be signed with Domain Keys Identified Mail (DKIM). The service SHOULD support MTA-STS, TLS-RPT and use opportunistic Transport Layer Security (TLS) in accordance with National Cyber Security Centre (NCSC) requirements on ciphers and certificates. All outbound connections to the public sector and business partners must use TLS in accordance with National Cyber Security Centre requirements on ciphers and certificates as soon as possible and by no later than **March 2020**. The commissioner of the email service must ensure adequate policies and / or contractual agreements are in place to safe guard this.	**PARTIALLY MET** Gmail provides advanced anti-virus, anti-malware, and anti-spam filtering, including alerting and blocking spoofed / lookalike domains. Gmail security sandbox mode helps protect against zero-day attacks in attachments. *It is the responsibility of each Organisation to configure their Google Workspace instance with advanced protection to comply with this (DCB1596) standard*: https://support.google.com/a/answer/7577854 Gmail supports DMARC, SPF and DKIM. MTA-STS and TLS-RPT are also supported. *It is the responsibility of each Organisation to configure Google Workspace appropriately to comply with this standard*: DCB1596 Secure Email - Google Workspace Implementation Guidance TLS connections can be enforced on a per-domain basis to meet the NCSC requirement for secured outbound connections to public sector / business partner organisations. *It is the responsibility of each Organisation to configure Google Workspace with appropriate TLS enforcement.*
7	All OFFICIAL data (particularly patient identifiable and OFFICIAL SENSITIVE) 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.	**MET** In line with ICO data protection principles, we provide a comprehensive guide for Google Workspace usage under GDPR: google_workspace_data_protection_guide_en_dec2020.pdf Google Workspace Administrators should ensure that the GDPR Compliance Amendments have been accepted for their domain:

		https://support.google.com/a/answer/2888485
8	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 (i.e. jail broken) devices.	**MET** Google Workspace provides a comprehensive range of Mobile Device Management (MDM) controls: https://support.google.com/a/answer/7576736 Google Workspace Business and Enterprise editions include all of the features listed in this section.
9	The Service Provider SHOULD provide eDiscovery tools to support the administration of the service, especially with respect to the EU General Data Protection Regulation, Data Protection Act 2018 and Freedom of Information Act 2000.	**MET** Google Vault (available for Google Workspace Business and Google Workspace Enterprise) lets you retain, hold, search, and export data to support your organization's archiving and eDiscovery needs: https://support.google.com/a/answer/2462365
10	Data must only be hosted in locations detailed in the NHS and social care off-shoring policy. Countries where data is hosted to be listed.	**MET** By default, data is hosted in either US (under Privacy Shield) or Europe. The Google Worskspace administrator can further constrain this policy to Europe or the US exclusively: https://support.google.com/a/answer/9223653 Google Workspace Data Centre locations for Europe and US: https://www.google.com/about/datacenters/inside/locations/index.html
Safety		
11	The email service MUST comply with the provisions of DCB0129: Clinical Risk Management: Its Application in the Manufacture of Health IT Systems.	**MET** Google Workspace has maintained compliance with DCB 0129 since the publication of the NHS DCB 1596. A Clinical Safety Case Report, and associated Clinical Risk Management Plan has been provided to support compliance.

Interoperability		
12	Each Service Provider SHOULD comply with the open standards policy.	**MET** Google is a strong believer in open standards. A full description of how Google engages with open standards and open-source projects is given here: https://cloud.google.com/open-cloud/
13	Each service provider MUST enable inbound and outbound opportunistic Transport Layer Security (TLS) version 1.2 or better for secure email transport between other secure email services.	**MET** Opportunistic TLS 1.3 is enabled by default for Gmail. Google actively promotes the deployment of TLS across email providers. Our Transparency Report publishes high level information on global TLS deployments. The Google Workspace Administrator can optionally enforce TLS domain wide, or for specific recipient domains, in line with NCSC policy: DCB1596 Secure Email - G Suite Implementation Guidance
14	TLS Ciphers should conform with current NCSC guidance.	**MET** Google Workspace supports a variation on the Foundation Profile for TLS given in the NCSC Guidance (December 2017). The guidance notes that "Deviation from this profile, such as through the use of GCM rather than CBC mode, or the use of Perfect Forward Secrecy (PFS), may be required or desirable, *and is acceptable*." [emphasis added] The TLS configuration will attempt to negotiate the highest security cipher suite that is mutually supported, to ensure that all communications are secured to the best of both sender and recipients ability. Workspace enforces a cipher suite order, to ensure that higher security ciphers are considered first. Google systems also support the TLS_FALLBACK_SCSV signal, which helps mitigate protocol downgrade attacks (such as POODLE).