DCB1596 Conformance Assessment:

Google Cloud
Date: 12th of September 2025
ICT Service Provider: Google Cloud EMEA Limited
Date of ICT Service Provider conformance: 12th of September 2025

Purpose

This document provides the results of a conformance assessment undertaken by NHS England 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 EMEA Limited** 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 EMEA Limited** Serviceassertions, 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 England 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 England 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.	Google implements a Business Continuity Plan (BCP) for our Services, and reviews and tests it at least annually and ensures it remains current with industry standards. In addition, information about how customers can use our Services in their own business contingency planning is available in our Disaster Recovery Planning Guide (https://cloud.google.com/architecture/dr-scenarios-planning-guide). Our detailed business continuity and redundancy plans are internal to Google and cannot be shared, however, the existence and operating effectiveness of these, is verified as part of our SOC 2/3 audit reports. https://cloud.google.com/security/compliance/soc-2. An independent third-party auditor has granted a formal certification, attestation, or audit report based on an assessment that affirms our compliance with ISO 22301:2019 - please see https://cloud.google.com/security/compliance/iso-22301 and https://services.google.com/fh/files/misc/fall_2024_google_gdc_iso_22301_certificate.pdf
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	Google Workspace is certified as ISO 27001 compliant and details of this can be viewed here. For more information on how Google Cloud handles Healthcare data in the UK please see our whitepaper on this For a reference to the published assessment please see the DSP Toolkit portal.

	Kingdom Accreditation Service (UKAS1) 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.	For a complete listing of our compliance offerings, please visit our compliance resource center.
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).	The Google Workspace email service (Gmail) is entirely within the scope of the Google Workspace ISO 27001 compliance certificate available from here. For a complete listing of our compliance offerings, please visit the compliance resource center.
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.	Google Cloud Platform, our common infrastructure, Google Workspace, and Chrome (Chrome Services, and Chrome Sync) are certified as ISO 27001 compliant. Google regularly reviews and updates where required our security policies which are endorsed and/or signed off from Google senior management team as required. NHS England has (as part of the accreditation process) also 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	An executive summary of the annual penetration test can be made available via your account team and will be sent directly to specific individuals at NHS England (provided an NDA is in place). Google hires an external auditor every year to review the security, confidentiality, integrity and

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

	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 England is sufficiently mitigated.	availability controls that are in place. Provided a suitable non-disclosure agreement or terms covering confidential information are in place , a copy of our SOC 2 audit report can be made available to NHS England. Google conducts 3rd party security penetration tests on a regular basis. Google has a security bounty program and offers rewards for vulnerabilities that are brought to our attention. Google uses a number of well-known third-party tools to scan its external perimeter on a regular basis for network vulnerabilities and configuration errors. These tools are also used internally on systems containing highly sensitive information. Additionally, Google undergoes yearly a third-party penetration test, by a qualified vendor, for both its external networks and financial-related applications. Organisations are not obliged to contact Google before undertaking penetration testing on their Google Cloud projects, provided the tests comply with the Acceptable Use Policy and Terms of Service. 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.	Gmail provides advanced anti-virus, anti-malware, and anti-spam filtering, attachment protection, spoofing protection, with helpful outcomes such as including warning, alerting and blocking. See more: https://support.google.com/a/answer/9157861 Email attachments can include malicious software that might be missed by traditional antivirus programs. To identify these threats,

	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.	Gmail can scan or run attachments in a virtual environment called Security Sandbox. See more: https://support.google.com/a/answer/7676854 Gmail also provides data loss prevention capabilities. See more: https://support.google.com/a/answer/6280516?hl=en Admins can increase Gmail security by turning on MTA Strict Transport Security (MTA-STS) with TLS-RPT for the domain. See more: https://support.google.com/a/answer/9261504 By default, Gmail always tries to use a secure (encrypted) TLS connection when sending email and this can be enforced on a per-domain basis to meet the NCSC requirement for secured outbound connections to public sector / business partner organisations. See more: https://support.google.com/a/answer/2520500 Admins and users can also Turn on Gmail Confidential Mode to protect sensitive messages from unauthorised access, for example, by requiring an SMS to be sent to the email recipient prior to releasing the message. See more: https://support.google.com/a/answer/7684332 You can also set up hosted Secure/Multipurpose Internet Mail Extensions (S/MIME) in your Google Workspace account to increase the security of your organisation's email. See more: https://support.google.com/a/answer/6374496?hl=en Gmail administrators should set up email authentication to protect their organisation's email using standards

		such as SPF, DKIM, DMARC. See set-up instructions here: https://support.google.com/a/answer/2466580 It is the responsibility of each Organisation to configure Google Workspace appropriately to comply with these standards.
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.	Data Protection In line with ICO data protection principles, we provide a comprehensive guide for Google Workspace usage under GDPR: https://services.google.com/fh/files/misc/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 Data Location By default, data is hosted globally in our data centres across North America, South America, Europe, and Asia: https://www.google.com/about/datacenters/inside/locations/index.html Google Workspace administrators can implement a data region policy to constrain covered data to either United States, or Europe, by toggling an option in the Admin Console: https://support.google.com/a/answer/9223653 For further data in-country data confidentiality, Client side encryption keys and near-term data backups can be stored in the country of organisation's choice outside of Google Workspace Infrastructure and only accessible

		by the customer (with granted permissions). See more: https://support.google.com/a/answer/10741897
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.	Google Workspace Enterprise editions provide a comprehensive range of Mobile Device Management (MDM) controls including and above those mentioned in the prompt. See here: https://support.google.com/a/answer/7576736 And here: https://support.google.com/a/answer/9852079
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.	Google Vault (available for Google Workspace Enterprise) lets you retain, old, search, and export data to support your organisation'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.	Data Location By default, data is hosted globally in our data centres across North America, South America, Europe, and Asia: https://www.google.com/about/datacenters/inside/locations/index.html Google Workspace administrators can implement a data region policy to constrain covered data to either United States, or Europe, by toggling an option in the Admin Console: https://support.google.com/a/answer/9223653 For further data in-country data confidentiality, Client side encryption keys and near-term data backups can be stored in the country of organisation's choice outside of Google Workspace

		Infrastructure and only accessible by the customer (with granted permissions). See more: https://support.google.com/a/answer/10741897
Safety		
11	The email service MUST comply with the provisions of DCB0129: Clinical Risk Management: Its Application in the Manufacture of Health IT Systems.	Google Workspace has maintained compliance with DCB 0129 since the publication of the NHS DCB 1596 standard. A Clinical Safety Case Report (including Hazard Log) has been provided to support compliance.
Interoperability		
12	Each Service Provider SHOULD comply with the open standards policy.	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.	Opportunistic TLS 1.3 is enabled by default for Gmail. Google Workspace supports TLS versions 1.0, 1.1, 1.2, and 1.3. More information here: https://support.google.com/a/answer/9795993 Google actively promotes the deployment of TLS across email providers. Our Transparency Report publishes high level information on global TLS deployments. More information here:https://transparencyreport.google.com/safer-email/overview
14	TLS Ciphers should conform with current NCSC guidance.	By default, Gmail always tries to use a secure (encrypted) TLS connection when sending email. 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 recipient's ability. See more: https://support.google.com/a/answer/9795993?hl=en This can be enforced on a per-domain basis to meet the NCSC

		requirement for secured outbound connections to public sector / business partner organisations. See more: https://support.google.com/a/answer/2520500