Google Cloud Whitepaper
January 2022

NTA 7516 for Gmail

Table of Contents

Disclaimer

This whitepaper applies to Gmail. The content contained herein is correct as of October 2021 and represents the status quo as of the time it was written. Google's security policies and systems may change going forward, as we continually improve protection for our customers.

Introduction

NTA 7516:2019 is ‘Requirements for safe email and chat applications’ (exchange of ad hoc messages with personal health information). This requirement has been published by NEN (the Royal Netherlands Standardization Institute). NTA 7516 focuses primarily on *ad hoc* messages between sender and receiver with highly sensitive medical information.

The standard is targeted at:

- Medical professionals sending or receiving medical information of patients via email
- Email software suppliers
- Patients whose information is being transferred

With this whitepaper, Google aims to help healthcare and medical professional customers navigate the NTA 7516 requirements and utilize the technologies employed by Gmail to help achieve compliance to the standard.

Path to compliance with NTA 7516 using Gmail

Gmail provides users with a cloud-based email system that is offered as part of Google Workspace.

The following is an overview of the key security capabilities that Gmail offers that could help medical professionals with their NTA 7516 obligations.

Overview of Gmail security, compliance, and the shared responsibility model

Gmail offers industry-leading security and infrastructure with comprehensive controls that can help our customers meet their objectives and satisfy the NEN requirements. Under the shared responsibility model, Gmail and our healthcare and medical professional customers share the management of the IT environment, including responsibilities for security. We work with our customers to delineate these responsibilities in an effective and transparent way.

Gmail's approach to security and data protection

Google's focus on security and protection of information is among our primary design criteria. In this section, we provide an overview of the organizational and technical controls we use to protect your data. To learn more about our approach to security and compliance, refer to the Google Cloud security and compliance whitepaper for Google Workspace.

Availability

Google's application and network architecture is designed for maximum reliability and uptime. Google owns and operates data centers around the world to keep the services you use running 24 hours a day, 7 days a week. So even if a machine—or even an entire data center—fails, your data will still be accessible.

To minimize service interruption due to hardware failures, natural disasters or other incidents, Google has built a highly redundant infrastructure of data centers. Google Workspace has an RPO (Recovery Point Objective) target of zero, and our RTO (Recovery Time Objective) target is instant failover (or zero).

Also, with Workspace, we offer a Service Level Agreement of 99.9% availability.

Integrity

Gmail supports the SPF, DKIM and DMARC frameworks for email services. These frameworks can be enabled so they're in use by default on the domain in the Google Workspace Admin console.

Gmail has the following authentication measures that are used to enhance integrity:

- A 2-step verification process for users including options for use of security keys

- Single sign-on (SAML 2.0)
- OAuth 2.0 and OpenID Connect

Gmail has SMTP MTA Strict Transport Security (MTA-STS), a mechanism enabling mail service providers (SPs) to both declare their ability to receive Transport Layer Security (TLS) secure SMTP connections and to specify whether sending SMTP servers should refuse to deliver to MX hosts that do not offer TLS with a trusted server certificate.

All of these controls can be enabled in the Google Workspace Admin Console for the entire domain.

Google encrypts customer data while it is "in transit"—traveling over the Internet and across the Google network between data centers by default. Workspace administrators can also enable S/MIME for messages with individual certificates for certain kinds of messages to enhance security.

Confidentiality

To ensure confidentiality, Google encrypts data as it is written to disk with a per-chunk encryption key that is associated with a specific Access Control List (ACL). The ACL ensures that data in each chunk can only be decrypted by authorized Google services and employees.

This means that different chunks are encrypted with different encryption keys, even if they belong to the same customer. These chunks are encrypted using the Advanced Encryption Standard (AES) cipher with a 128-bit or stronger key.

The decryption key for the per-medium secret is known only to the Key Management System (KMS) and never leaves it. In addition, it's only the backup service that has permission to ask the KMS to decrypt a per-medium secret.

This provides a double layer of access control in that:

(1) Only authorized personnel and services may read seeds from the backup system's database

(2) A further authorization check is required to use such a seed to ask the KMS to decrypt a per-medium secret. This additional check provides a further protection against modification of data on a backup medium.

With Gmail having the 2-step verification with security key options, Single Sign-on (SAML 2.0), and OAuth 2.0 and OpenID Connect, there is an additional layer of confidentiality protection based on authorized user access.

Gmail also has SMTP MTA Strict Transport Security (MTA-STS). As discussed above, this is a mechanism that enables mail service providers (SPs) to declare their ability to receive Transport Layer Security (TLS) secure SMTP connections and to specify whether sending SMTP servers should refuse to deliver to MX hosts that do not offer TLS with a trusted server certificate. All of this can be enabled in the Google Workspace Admin Console for the entire domain.

While customer data in transit over the internet across the Google Network is encrypted for confidentiality between data centers by default, Workspace administrators can also enable S/MIME for messages with individual certificates for certain kinds of messages to enhance confidentiality.

Gmail supports SPF, STARTTLS, DKIM and DMARC for email services and has support articles on how to set those up for each domain.

Google offers to sign the Data Processing Amendment for Google Workspace. Google Cloud also offers Standard Contractual Clauses or Model Contract Clauses (MCCs) to our customers, which are already incorporated in our DPA. If the GDPR applies to customers' use of Gmail, the MCCs will automatically apply as part of the DPA. Gmail, through Google Workspaces, is certified for ISO/IEC 27701 which is a global privacy standard that focuses on the collection and processing of personally identifiable information (PII).

User-Friendly

Gmail offers an encryption check to confirm that the message received is encrypted. The user can verify with a simple step. When replying to emails, Gmail will encrypt the message with the same security. Also, in the Compose field, the user can view the encryption supported by the recipient email servers.

The recipient can also see from the email who exactly the email has come from and which domain. If Gmail cannot verify who the email has come from, it puts a question mark next to the sender's name. This helps alert the user to potential threats.

Gmail supports forwarding of Emails to other parties, however a sender can also prevent forwarding or downloading of the email using Gmail confidential mode.

Gmail is browser-based and all emails are readable on the browser that is used to open and authenticate the emails.

To improve the user's experience, Google requires all public facing products to meet a minimum accessibility requirement. Gmail offers support for accessibility with screen readers through Chrome, keyboard shortcuts, themes with higher contrast and configurable buttons with text rather than icons.

Additionally Gmail offers Workspace tools such as Google Docs and Google Sheets that can enable a user to open attachments in the browser itself without requiring additional software.

Emails on Gmail can be downloaded to a computer or exported as required by the user.

To support our users, we regularly update and provide support pages for Gmail to both basic and advanced users. For the Workspace Administrators further help is available for what they can configure for their domain as well as an active community page where they can interact with other users to obtain help and support.

Interoperability

Each email thread has a unique url that can be linked. However, to maintain the security of the email and its contents, the email url is different for the recipient and the sender and only the user whose unique url is linked can view the email after authentication.

Administrators can enable Gmail confidential mode that by default secures all outgoing emails and requires the recipient to login to a dedicated page to access the message. This alone, however, will not satisfy the NTA 7516 requirement. To achieve true NTA7516 interoperability, a third-party plugin such as Zivver can be used to ensure that emails to NTA 7516 certified recipients can be sent as a regular email.

Activity logs for the domain can be accessed by the administrator through the console.

Gmail’s approach to compliance

Industry Certifications & Independent Third-party Audits and Attestations

Gmail regularly undergoes independent verification of security, privacy, and compliance controls, achieving certifications against global standards to earn the trust of our customers. We are constantly working to expand our coverage. For more information, refer to our compliance resource center.

Based on the requirements of NTA 7516 and the privacy related aspects of the medical sector, we adhere to the following relevant standards and have the following certifications:

ISO 27001 (Information Security Management)

The International Organization for Standardization 27001 (ISO 27001) is one of the most widely recognized, internationally accepted security standards; it outlines and provides the requirements for an information security management system (ISMS). The ISO 27001 lays out a framework and checklist of controls that allows Google to ensure a comprehensive and continually improving model for security management. Gmail being part of Google Workspace is certified as ISO 27001 compliant.

Additionally a mapping of the ISO 27001 to NEN 7510 can be referenced.

ISO 27017 (Cloud Security)

The International Organization for Standardization 27017 (ISO/IEC 27017:2015) gives guidelines for information security controls applicable to the provision and use of cloud services by providing additional implementation guidelines for relevant controls specified in ISO/IEC 27002 and more controls with implementation guidelines that specifically relate to cloud services. This standard provides controls and implementation guidelines for both cloud service providers (like Google) and our cloud service customers. Gmail being part of Google Workspace is certified as ISO 27017 compliant.

ISO 27018 (Cloud Privacy)

The International Organization for Standardization 27018 (ISO 27018) is an international standard of practice for protection of personally identifiable information (PII) in Public Cloud Services. This standard primarily focuses on security controls for public cloud service providers acting as PII processors. Gmail being part of Google Workspace is certified as ISO 27018 compliant.

ISO 27701 (Cloud Privacy)

The International Organization for Standardization 27701 (ISO 27701) is an international standard that provides guidance for establishing, implementing, maintaining and continually improving a Privacy Information Management System (PIMS). Gmail being part of Google Workspace is certified as ISO 27701 compliant. Gmail is the first hyperscale email provider to achieve this certification.

Security & Regulatory Compliance Specialists

Google Cloud has a dedicated compliance team that reviews compliance with security laws and regulations around the world. As new frameworks are created, the Compliance team determines what controls, processes, and systems are needed to meet them. This team facilitates and supports independent audits and assessments by third parties. In addition, Google contractually commits to the following:

- We will maintain adherence to ISO 27001, ISO 27017, ISO 27018 and ISO 27701 audits during the term of the agreement.
- We will define how data is protected through specific defined security standards.
- Customers may contact Google's Cloud Data Protection Team for questions or comments.

Conclusion

Google designed Google Workspace to meet stringent privacy and security standards based on industry best practices. With this in mind, Gmail was designed to be secure and available to our customers. As we maintain compliance to standards such as ISO 27001 we continue to provide assurance to our customers requiring NTA 7516 compliance that Gmail will support you in your efforts to help keep your data secure.

Furthermore, because protecting data is core to Google Workspace, we can make extensive investments in security, resources and expertise at a scale that others cannot. Our investment frees you to focus on your business and innovation.