Microsoft

Microsoft Intune privacy and data protection overview

August 2015

Privacy and data protection overview

The Microsoft Intune service can help organizations manage and secure mobile devices, applications, and PCs across Windows, Windows Phone, Apple iOS, and Google Android platforms. Because it is cloud-based and hosted in Microsoft's data centers, Intune requires no additional infrastructure, but organizations can use the service to extend existing management infrastructure into the cloud. In addition to enhancing device security by providing update and policy management, Intune can help organizations give employees access on their own devices to the apps and resources they need, making Bring Your Own Device (BYOD) programs a reality.

Relying on Microsoft Intune to manage organizations' devices requires trust, but before customers give that trust, they want to know the answer to questions like:

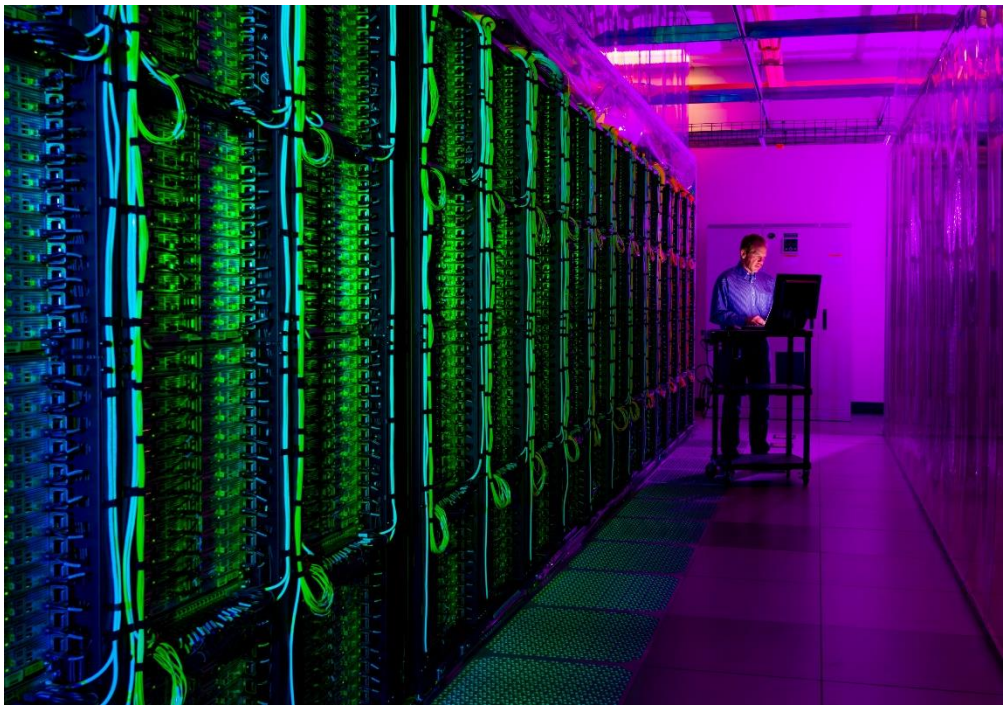
- Who can access their data and how do we use it?
- Where does Microsoft store their data?
- How is their data secured in the data center and on the move?
- Is the privacy of their data assured, and who owns their data?
- What organizations have independently verified Microsoft Intune?

Microsoft takes its responsibility to protect customers' data seriously, and we are committed to providing the answers you need to trust Intune. We have applied our many years of cloud and on-premises experience with security and privacy to our management of Intune.

This white paper offers an overview of how we help secure your data and protect its privacy. Of course, the technical details in this white paper are subject to change, but our commitment to the protection of your data and devices will not waver.

Physical security

Security for the service starts in the data center. The Microsoft Cloud Infrastructure and Operations Group (MCIO) delivers the core infrastructure and foundational technologies for Microsoft's more than 200 online businesses, including Bing, Hotmail, MSN, Microsoft Office 365, Xbox Live, and the Microsoft Azure platform. MCIO hosts Microsoft Intune in its data centers, which are strategically located around the world. It brings all of this experience to Intune.



MCIO controls personnel's physical access to data centers by using two-tier authentication, including proxy card access readers and biometric readers. On a quarterly basis, a Microsoft security officer sends reports to personnel with authority to approve data center access. Authorized personnel regularly review the list to verify that all people on that list still require access and have the least privileged access level necessary to perform their job functions.

Respected non-Microsoft registrars and accreditation organizations regularly audit MCIO data centers in support of the various certifications MCIO undertakes for the data centers.

These include:

- ISO/IEC 27001:2005
- SSAE 16/ISAE 3402 (Service Organization Control [SOC] 1, SOC 2, SOC 3)
- FISMA
- PCI data security standard

Microsoft recognizes that security is an ongoing process, not a steady state. Therefore, experienced and trained personnel constantly maintain, enhance, and verify our infrastructure. We use up-to-date software, hardware technologies, and processes for designing, building, operating, and supporting our services. To learn more about MCIO, visit http://www.microsoft.com/datacenters

Personnel security

Security starts with people, and Intune is no exception. Beginning with the hiring process, all U.S.-based Microsoft employees and subcontractors with access to customer data go through standard background checks as permitted by law, which include a review of candidates' education, employment, and criminal history. In addition to standard background checks for all new personnel, personnel must undergo

additional background checks if they are to have access to customer data or manage key physical or logical access controls. Additional verification includes checks against export control lists, such as the Office of Foreign Assets Control List, the Bureau of Industry and Security List, and the Directorate of Defense Trade Controls Debarred Parties List. To protect the privacy of its employees and subcontractors, Microsoft does not share the results of background checks with customers.

Security awareness, data protection, and privacy are key topics of this training. Microsoft also requires that all personnel complete business conduct training each year.

We follow principles of segregation of duties and least privilege. Although physical access to data centers is generally limited to MCIO staff, select Microsoft Intune personnel have logical access to the Microsoft Intune service and data hosted in the data centers. Employees are accountable for their handling of customer data. Microsoft enforces this accountability through a process that includes system controls, such as the use of unique user names, role-based access, and two-factor authentication (e.g., smartcards and Rivest Shamir Adleman [RSA] tokens). As with physical access to the data centers, we review logical access periodically to help ensure that only appropriate access is granted to customer data, such as contact information, computer details, and user information.

Architecture security

The following sections offer an overview of security for architectural components, including:

- Client installation and enrollment on PCs
- Mobile devices, such as Windows Phone
- Account, Administrator, and Company Portals
- Identity and authentication
- Microsoft System Center 2012 Configuration Manager

Client installation and enrollment on PCs

The PC enrollment process is documented in the article "Manage computers with Microsoft Intune" at http://technet.microsoft.com/library/dn646959.aspx. Only a customer's Intune administrator can use the Administrator portal to download client software. End users with existing Intune accounts can download and install client software from the Company Portal after they complete the self-enrollment process.

Client installation requires elevated permissions, which helps protect the PC from malicious installation. (You can deploy the client software to standard users by using Group Policy or an electronic software distribution [ESD] system like System Center 2012 Configuration Manager.) If organizations choose to distribute the client software by using a file share or an ESD system, they should take steps to prevent unauthorized access

to it (e.g., use access control lists to secure it)

Mobile devices

Each mobile platform uses their own proprietary processes and security models to help secure client installation on mobile devices. E.g., the security measures of the Windows Store, Google Play, and Apple App Store contribute to the security of the client software. Microsoft follows the rules each store has set up for publishing our Company Portal apps into them.

For Windows Phone, Android, and iOS mobile devices, Microsoft uses Secure Sockets Layer (SSL) to help secure communication between each device and the Intune service. Intune communicates with iOS devices by using the Apple Notification Service. Intune uses a certificate, which the administrator must download from the Apple Push Certificates Portal, to talk to the Apple Mobile Device Management service. For Windows Phone and Windows RT devices, it uses the Windows Notification Service and for Android devices, Google Cloud Messaging is used. For more information about planning and setting up management of mobile devices, see this article on TechNet: https://technet.microsoft.com/library/dn646962.aspx.

Account, Administrator, and Company Portals

Intune provides the following portals:

Account portal This portal provides the service and user account management interface to the Intune online service. The account Administrator uses this portal to manage user accounts, user groups, domain names, passwords (if configured), and subscriptions for the Intune service.

Administrator console The Administrator console enables administrators to set policies, upload software and software updates, and manage PCs remotely.

Company portal Users can see machine status, download software, and contact their company's IT support through the web-based Company Portal. To access the Company Portal, a user must be granted access by the administrator and enroll their device.

All three portals use SSL to secure communication with the web browser. Sessions have an inactivity timeout—that is, after a period of no activity, the user's session is ended, and the user must sign into the portal again.

NOTE Organizations can configure the Remember Me option in Active Directory Federation Services (AD FS) to automatically sign users in for a specific timeframe. This configuration supersedes the total timeout in Intune.

Identity and authentication

Intune uses Azure Active Directory (Azure AD) as its authentication platform. To provide users with a single sign-on (SSO) experience, businesses can connect their on-premises directories with Azure AD. The Intune administrator then adds users to the Intune user group, giving them seamless access to Intune when they sign into the corporate network. There are two options for authentication when connected to Azure AD: Federation with AD FS and Password Sync. With AD FS, users' credentials never leave the domain network while with Password Sync the hash of users' passwords is synchronized to the cloud.

Use the latest directory integration tools from Microsoft in order to configure single sign for Intune. For more information about connecting on-premises directories to the cloud, see this article at

https://azure.microsoft.com/documentation/articles/active-directory-aadconnect

For organizations that do not want single sign on, they can create cloud only users and administrators in Azure AD. For more information about creating cloud only users, see this article at https://technet.microsoft.com/library/dn646967.aspx#Step1

System Center 2012 Configuration Manager

Organizations can integrate Intune with System Center 2012 Configuration Manager Service Pack 1 and more recent product versions.

This combination helps provide a unified device management solution that focuses on users and the variety of devices they employ to get their work done.

In this hybrid configuration, the System Center 2012 Configuration Manager site initiates all communication with Intune to push or pull data to the service. For example, Intune queues messages for System Center 2012 Configuration Manager, and the site uploads or downloads them. Intune does not initiate communications with System Center 2012 Configuration Manager.

All communications are over SSL. An Intune certificate is installed with the Intune Connector role and the site uses that certificate to authenticate and communicate with the connector. Intune client software is not aware that Intune is using a hybrid configuration. The data flow is the same whether the client software is installed on a PC or a mobile device, but the data being distributed to the device depends on the feature being used (e.g., software distribution versus policy enforcement).

Data flow between the on-premises site and Microsoft Intune

From Microsoft Intune to the System Center 2012 Configuration Manager site Data that Intune delivers to System Center 2012 Configuration Manager includes detailed inventory information that devices report, such as installed apps and hardware characteristics. Intune packages and forwards this information to the System Center 2012 Configuration Manager site. System Center 2012 Configuration Manager maintains the detailed information about organizations' devices and users in the customer's own data centers.

From the System Center 2012 Configuration Manager site to Microsoft Intune The System Center 2012 Configuration Manager site uses the Intune Connector to upload relevant data and policies to the Intune service.

When necessary, Intune caches data for optimal transport (for example, caching data for mobile devices when using metered connections). The service flushes data from the cache after a set period. For more information, see this article on TechNet: http://technet.microsoft.com/library/dn823755

Privacy

Customer Data is defined as "all data, including all text, sound, video or image files, and software that are provided to Microsoft by, or on behalf of, Customer through use of the Online Service." For example, this includes inventory information from managed devices or apps which have been installed through Intune. Customers can access their own Customer Data at any at any time and for any reason without assistance from Microsoft. Microsoft will not

use Customer Data or derive information from it for advertising. We will use Customer Data only to provide the service or for purposes compatible with providing the service.

It is ultimately up to our customers to evaluate our offerings against their own requirements, so they can determine if our services satisfy their regulatory needs. We are committed to providing our customers detailed information about our cloud services to help them make their own regulatory assessments.

Microsoft does not create customer accounts; the customer creates the accounts either directly in Intune Administrator Console, or in their local Active Directory, where the accounts can then be synchronized into Azure Active Directory. For this reason, the customer remains responsible for the accuracy of the user accounts they created.

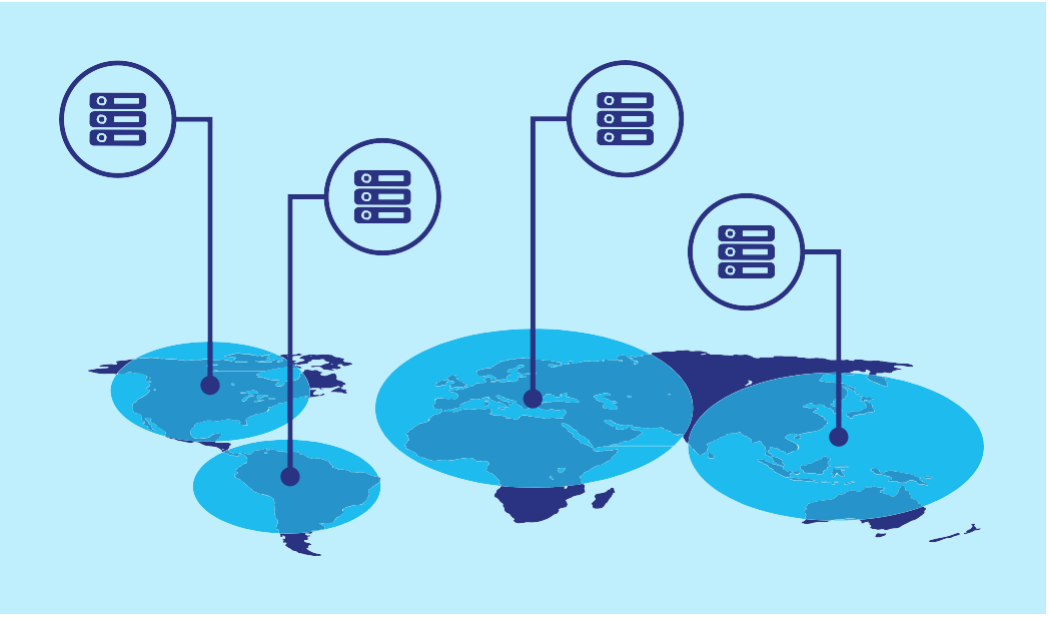
Microsoft provides a coherent, robust, and transparent privacy policy that emphasizes customer data ownership. The Microsoft Online Services Privacy Statement tells you how we handle and use data gathered in your company's interactions with the Intune service. You can view this Privacy Statement at http://go.microsoft.com/fwlink/?LinkId=512132.

The following list summarizes Microsoft's position on customers' privacy:

- Microsoft respects the privacy of your Customer Data.
- Microsoft does not mine your data to create advertisement products.
- Microsoft believes that Customer Data belongs to the customer.
- Microsoft does not mingle your data.
- Microsoft will not contact you unless we have your permission or it is regarding your service.

Intune enables customers to publish company privacy statements to their end users.

For more information about customizing company privacy statements, see the article "Start using Microsoft Intune" at http://technet.microsoft.com/library/dn646983.aspx



Data protection

Intune collects customer data only to provide and trouble-shoot the service. Data the Intune service collects includes:

- Device names and inventory data used to provide the service.
- Administrator data, including the name, address, phone number, and email address of the account owner and IT administrators (Microsoft uses this data to provide the Online Service, complete transactions, administer the

account and detect and prevent fraud.)

There are three types of data collected from mobile devices managed by Intune:

1. Hardware inventory This information is provided by the mobile device operating system (Windows, iOS, and Android) and may be different based on each OS. Such information could include:

- Name
- Manufacturer
- Model
- Operating system
- Processor
- Serial number
- OS version
- Cellular technology
- Jailbreak status
- Free/Total space
- Exchange Device ID
- Wi-Fi MAC address
- Ethernet MAC address
- Device encryption status

2. App inventory There are two types of apps which can be installed on a mobile device. Corporate apps are installed through Intune's Company Portal and are offered or required by your company's Intune administrator. Personal apps are those which the user installs on their own from the Windows Store, Apple App Store, or Google Play.

App Inventory includes:

- Name
- Version
- ID
- Installation location
- Size

There are a few factors which affect which apps are inventoried.

Personal or corporate-owned devices When Intune manages a mobile device, it assumes the device is personally-owned. In the hybrid model where Intune is connected to System Center Configuration Manager, the administrator can identify specific devices as corporate-owned. By default, on personal devices, only those apps which are installed via Intune and the Company Portal are inventoried, whereas on corporate devices, all apps are inventoried.

Compliant and non-compliant apps When the administrator defines compliant and non-compliant apps to define which apps are allowed on a device in order to be considered "compliant" with corporate policies, it is necessary to inventory all apps, even on a personal device, to compare against the policies. **These personal apps are listed in reports available to the Intune administrators.**

3. Policies and configurations Device or application management settings, certificates, VPN and Wi-Fi profiles are all examples of policies and configurations which an Intune administrator can define and deploy. This content, as well as the resulting compliance information from each managed device, is also stored by Intune.

Intune does not collect information specific to user activities, including:

- Phone logs
- Contacts, email, calendar information
- Documents
- Text (SMS) messages
- Video/photos
- GPS information
- Web browsing history

Data locality

Microsoft has a regionalized data center strategy. The customer's country or region, which the customer's administrator inputs during initial setup of the services, determines the primary storage location for that customer's data. For example, if a customer in the United Kingdom creates an Intune subscription, their subscription will be created and customer data stored in a Microsoft data center located in a European Union (EU) country.

To help ensure service availability, Intune follows a business continuity methodology that enables data center failover within a given region:

Primary data centers A primary data center is where the application software and customer data running on the software are located. For all customers located in North America, the primary data centers are located in United States. If North American customers access their Microsoft Intune subscriptions from another region, such as the European Union, they will still be using data stored in North America. If you subscribe to Intune from a region other than North America, then the web pages and data you view will be hosted in that region's data center.

Backup data centers A backup data center is used for failover purposes. All primary data centers have backup data centers in the same region. If the primary data center ceases to function for any reason, the service is designed to make the application software and customer data available from the backup data center. Customers might not be notified when failover occurs. Depending on the particular service that fails, failover may not result in service interruption.

Data disposition

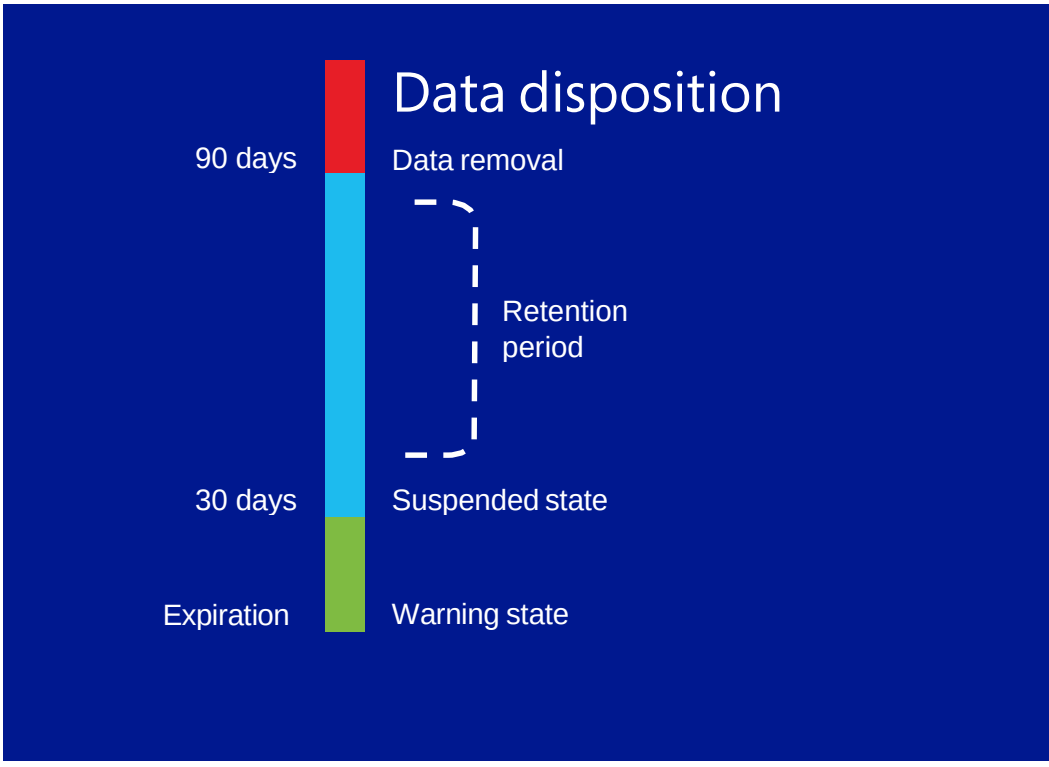
Microsoft believes that customers own their own data. When customers do not renew their Microsoft Intune subscriptions (i.e., they terminate or allow their subscriptions to expire), their subscriptions move through the following states:

Warning state Their subscriptions initially go into a warning state during which they can continue to use the service and their Customer Data is available. They have 30 days to renew their subscriptions, and during this time they will receive notifications.

Suspended state If after 30 days customers do not renew their subscription, they go into the suspended state. They still have rights to their Customer Data and can continue accessing the service, but they cannot enroll any new devices into the service.

Retention period At the end of the Suspended state, customers can continue accessing their Customer Data for 90 days in a limited function. If after 90 days customers do not renew their subscription, Customer Data is removed within 30 days of the end of the retention period.

Customers who actively cancel their subscription may choose to disable their accounts and request deletion of their



subscriber data by contacting our Customer Support team. If they do not provide specific instructions to delete their data, we follow the 90 day retention period. There is no 30 day suspend state or warning. At the end of the 90 day retention period, Intune removes Customers Data within 30 days of the end of the retention period.

Independent verification

Intune is compliant with many world-class industry standards, and it is verified by third parties. Independent verification of Intune includes:

Certified for International Organization for Standardization (ISO) 27001 ISO 27001 is one of the best security benchmarks available across the world.
Intune has implemented the rigorous set of physical, logical, process, and management controls ISO 27001 defines. Intune has also adopted the uniform international code of practice for cloud privacy, ISO/IEC 27018, which governs the processing of personal information by cloud service providers. ISO 27018 is the first international set of privacy controls in the cloud and Microsoft was the first to adopt its code of practice.

US to EU Safe Harbor and EU Model Clauses Intune is certified in the US-EU Safe Harbor Framework, which is an agreement between the United States and the European Union that enables organizations to self-certify compliance with data protection requirements regarding the collection, use and retention of data to allow legal data transfer from the EU to the U.S. In addition to being certified under EU Safe Harbor, Microsoft offers Intune customers EU "Model Clauses" which are standardized contractual clauses that provide contractual guarantees around transfers of personal data leaving the European Economic Area (EEA).

Microsoft is the first company to receive a letter of endorsement and joint approval from the EU's Article 29 Working Party, which includes data protection authorities from each of the EU member states, for its strong contractual commitments to comply with EU data protection laws regarding the international transfer of data. This recognition applies to Microsoft's enterprise cloud services – in particular, Microsoft Azure, Office 365, Microsoft Dynamics CRM and Microsoft Intune. Learn more.

Statements on Standards for Attestation Engagements No. 16 (SSAE 16) SSAE 16, the successor to Statement on Auditing Standards (SAS) 70, and International Standards for

Attestation Engagement No. 3402 (ISAE 3402) are audit standards established by the American Institute of Certified Public Accountants and the International Auditing and Assurance Standards Board of the International Federation of Accountants, respectively, and are geared toward service organizations – typically entities that provide outsourcing services that affect the control environment of their customers.

Examples of service organizations are insurance and medical claims processors, hosted data centers, application service providers, and managed security providers. SSAE 16 and ISAE 3402 audits are independent verifications of compliance with and effectiveness of security controls.

At the conclusion of an SSAE 16/ ISAE 3402 service auditor's examination ("SSAE 16 audit"), the service auditor renders an opinion on the following information:

- Whether the service organization's description of

controls is presented fairly

- Whether the service organization's controls are designed effectively
- Whether the service organization's controls are placed in operation as of a specified date

Microsoft's SSAE 16/ISAE 3402 audits are conducted once per year by an external third party (one of the "Big Four" accounting firms).

The audit report produced includes an opinion of the controls by the external third party. Intune has undergone SSAE 16 (Service Organization Control [SOC] 1, SOC 2, SOC 3) Type I and Type II audits. For more information about the standard and types of audits, go to www.aicpa.org.

MCIO provides infrastructure services (data centers and networking) for both Microsoft itself (including the Intune service) and its customers. MCIO is SSAE 16 (SOC 1, SOC 2, SOC 3) Type II certified today. The SSAE 16 report for Microsoft Intune represents the application layer controls for the service. Together with the MCIO report pertaining to the infrastructure layer, the audit reports provide an end-to-end representation of controls in place.

Health Insurance Portability and Accountability Act (HIPAA) Business Associate Agreement (HIPAA BAA)

HIPAA is a U.S. law that applies to health care entities that governs the use, disclosure, and safeguarding of protected health information (PHI) and imposes requirements on covered entities to sign BAAs with their vendors that use and disclose PHI. To help Intune customers comply with HIPAA, Microsoft offers a HIPAA BAA to Intune customers who have a Volume Licensing / Enterprise Agreement (EA).

UK Government G-Cloud

G-Cloud is a U.K. Government initiative and Procurement Framework to promote government-wide adoption of cloud computing. The G-Cloud Framework includes a Digital Marketplace where public-sector organizations and eligible government-funded independent organizations can compare and procure cloud-based services.

Microsoft Intune is compliant with the 14 Cloud Security Principles, followed by a sampled verification audit performed by the UK Government Digital Service (GDS), a branch of the Cabinet Office. Intune is available to UK Government customers under the latest version of the G-Cloud Framework (v6). As such, UK Government customers can utilize Intune to store and process OFFICIAL data, which makes up the vast majority of UK Government data.

Intune customers throughout the world are subject to many different laws and regulations. Legal requirements in one country or industry may be inconsistent with legal requirements applicable elsewhere. As a provider of global cloud services, Microsoft runs its services with common operational practices and features across multiple jurisdictions. To help customers comply with their own requirements, Microsoft builds its services with common privacy and security requirements in mind, and our built-in capabilities help customers comply with a wide range of regulations. It is ultimately up to customers to evaluate our offerings against their own requirements, so they can determine whether Intune satisfies their legal and regulatory needs.

Conclusion

Intune can help any business reduce the cost and complexity of managing PCs, mobile devices, and applications. It can even help businesses adapt to entirely new scenarios, such as BYOD. But no business can move management into a cloud-based service without understanding its security practices and technologies.

To that end, Microsoft built Intune to meet the high bar required to gain business' confidence and trust. Microsoft built the service leveraging its years of experience providing sophisticated cloud and on-premises solutions. Intune makes it easy for businesses to access and use its services while helping keep their data private and secure in its data centers. To learn more about Intune, visit http://www.microsoft.com/intune

Additional resources

To learn more about Intune security in the data center, see:

- Microsoft Intune Trust Center Frequently Asked Questions at http://aka.ms/intunetrustcenterfaq
- Microsoft Online Services at http://www.microsoft.com/online
- Microsoft MCIO at http://www.microsoft.com/datacenters
- Microsoft Trustworthy Computing at http://www.microsoft.com/twc

Microsoft Intune