# HIPAA and the HITECH Act United States

Microsoft offers Health Insurance Portability & Accountability Act Business Associate Agreements (BAAs).

## Microsoft and HIPAA and the HITECH Act

HIPAA regulations require that covered entities and their business associates—in this case, Microsoft when it provides services, including cloud services, to covered entities—enter into contracts to ensure that those business associates will adequately protect PHI. These contracts, or BAAs, clarify and limit how the business associate can handle PHI, and set forth each party's adherence to the security and privacy provisions set forth in HIPAA and the HITECH Act. Once a BAA is in place, Microsoft customers—covered entities—can use its services to process and store PHI.

Currently there is no official certification for HIPAA or HITECH Act compliance. However, those Microsoft services covered under the BAA have undergone audits conducted by accredited independent auditors for the Microsoft ISO/IEC 27001 certification.

Microsoft enterprise cloud services are also covered by FedRAMP assessments. Microsoft Azure and Azure Government received a Provisional Authority to Operate from the FedRAMP Joint Authorization Board; Microsoft Dynamics 365 U.S. Government received an Agency Authority to Operate from the US Department of Housing and Urban Development, as did Microsoft Office 365 U.S. Government from the US Department of Health and Human Services.

## Microsoft in-scope cloud services

- Azure, Azure Government, and Azure DevOps: Learn more
- Cloud App Security
- Dynamics 365 and Dynamics 365 U.S. Government: Learn more
- Flow cloud service either as a standalone service or in an Office 365 or Dynamics 365 branded plan or suite
- Health Bot Service
- Intune
- Microsoft Professional Services: Premier and On Premises for Azure, Dynamics 365, Intune, and for medium business and enterprise customers of Office 365
- Office 365, Office 365 U.S. Government, and Office 365 U.S. Government Defense: Learn more
- PowerApps cloud service either as a standalone service or in an Office 365 or Dynamics 365 branded plan or suite
- Power BI cloud service either as a standalone service or in an Office 365 or Dynamics 365 branded plan or suite
- Stream

## Audits, reports, and certificates

Microsoft Health Bot HIPAA Security and Privacy Compliance Assessment

## How to implement

- **Azure HIPAA/HITRUST Blueprint**
  Tools and guidance to help accelerate your deployment of HIPAA and HITRUST solutions on Azure. Learn more
- **Azure HIPAA/HITECH guide**
  Concrete steps to help you maintain compliance as you implement HIPAA and HITECH Act requirements. Learn more
- **Dynamics 365 & Office 365 HIPAA/HITECH guide**
  Concrete steps to help you maintain compliance as you implement HIPAA and HITECH Act requirements. Learn more
- **Designing secure health solutions**
  Practical guide using Azure to successfully adopt a cloud service in a secure manner. Learn more

- **Addressing HIPAA requirements**
  Guidance on building Microsoft Cloud solutions that comply with HIPAA security and privacy requirements.
  Learn more

## About HIPAA and the HITECH Act

The Health Insurance Portability and Accountability Act (HIPAA) is a US healthcare law that establishes requirements for the use, disclosure, and safeguarding of individually identifiable health information. It applies to covered entities—doctors' offices, hospitals, health insurers, and other healthcare companies—with access to patients' protected health information (PHI), as well as to business associates, such as cloud service and IT providers, that process PHI on their behalf. (Most covered entities do not carry out functions such as claims or data processing on their own; they rely on business associates to do so.)

The law regulates the use and dissemination of PHI in four general areas:

- Privacy, which covers patient confidentiality.
- Security, which deals with the protection of information, including physical, technological, and administrative safeguards.
- Identifiers, which are the types of information that cannot be released if collected for research purposes.
- Codes for electronic transmission of data in healthcare-related transactions, including eligibility and insurance claims and payments.

The scope of HIPAA was extended with the enactment of the Health Information Technology for Economic and Clinical Health (HITECH) Act. Together, HIPAA and HITECH Act rules include:

- The HIPAA Privacy Rule, which focuses on the right of individuals to control the use of their personal information, and covers the confidentiality of PHI, limiting its use and disclosure.
- The HIPAA Security Rule, which sets the standards for administrative, technical, and physical safeguards to protect electronic PHI from unauthorized access, use, and disclosure. It also includes such organizational requirements as Business Associate Agreements (BAAs).
- The HITECH Breach Notification Final Rule, which requires giving notice to individuals and the government when a breach of unsecured PHI occurs.

## Frequently asked questions

**Can my organization enter into a BAA with Microsoft?**

Microsoft offers qualified companies or their suppliers a BAA that covers in-scope Microsoft services.

- For Microsoft cloud services: The HIPAA Business Associate Agreement is available through the Online Services Terms by default to all customers who are covered entities or business associates under HIPAA. See "Microsoft in-scope cloud services" above for the list of cloud services covered by this BAA.
- For Microsoft Professional Services: The HIPAA Business Associate Amendment is available for in-scope Microsoft Professional Services upon request to your Microsoft services representative.

**Does having a BAA with Microsoft ensure my organization's compliance with HIPAA and the HITECH Act?**

No. By offering a BAA, Microsoft helps support your HIPAA compliance, but using Microsoft services does not on its own achieve it. Your organization is responsible for ensuring that you have an adequate compliance program and internal processes in place, and that your particular use of Microsoft services aligns with HIPAA and the HITECH Act.

**Can Microsoft modify my organization's BAA?**

Microsoft cannot modify the HIPAA BAA because Microsoft services are consistent for all customers and so must follow the same procedures for everyone. However, to create the BAA for our HIPAA-regulated customers and its services, Microsoft collaborated with some of the leading US medical schools and their HIPAA privacy counsel, as well as other public- and private-sector HIPAA-covered entities.

## Additional resources

- HIPAA Omnibus Final Rule
- Microsoft and FedRAMP
- Understanding HIPAA Compliance with Azure
- Microsoft Cloud for Government