EMPOWERING
HEALTH

YOUR COMPLIANCE,
YOUR WAY
Get flexibility and choice with your HIPAA BAA

Leslie Sistla
CISO, Worldwide Health Industry | Microsoft

June 2016

For the latest information, please see www.microsoft.com/health
## CONTENTS

1. OVERVIEW ............................................................................................................................................................................. 3

2. A STRONG HISTORY OF COLLABORATION .......................................................................................................................... 4

3. MOST HIPAA BAA-COVERED CLOUD SERVICES ................................................................................................................ 4

4. STREAMLINED, SELF-SERVICE PROCESSES ......................................................................................................................... 5

5. FLEXIBILITY TO IMPLEMENT SECURITY YOUR WAY ............................................................................................................. 6

6. OPERATIONALIZED COMPLIANCE ........................................................................................................................................ 6

7. CLOUD PRINCIPLES OF TRUST ............................................................................................................................................. 7

8. END-TO-END PROTECTION FOR TODAY’S WORLD .................................................................................................................... 7

9. INVESTING HEAVILY IN YOUR SECURITY .............................................................................................................................. 9

10. COMMITTED TO YOUR COMPLIANCE ................................................................................................................................ 9
A HIPAA BAA THAT SUPPORTS YOUR DIGITAL TRANSFORMATION

1. OVERVIEW
As a health organization, you know you need a Health Insurance Portability and Accountability Act (HIPAA) Business Associates Agreement (BAA) with cloud vendors. It’s mandated by law. HIPAA regulations require that covered entities and their business associates enter into written agreements with their service providers who provide certain functions using individually identifiable health information—such as cloud services that store and process protected health information (PHI).

But you also want to be able to meet your compliance requirements your way. And you need a wide range of services to choose from to support your digital transformation. So you want a HIPAA BAA that enables flexibility and choice.

Enter the Microsoft HIPAA BAA. We offer more covered services than any other cloud vendor under one umbrella HIPAA BAA. We’re continually adding more cloud services and streamlining processes for our customers. And you can implement solutions and security your way.

Plus, with Microsoft, you benefit from end-to-end trusted technology. And you can empower people with familiar tools they already know how to use—so you can worry less about your staff turning to shadow IT that can put you at risk for security vulnerabilities and compliance violations.

All of this is important because you also know that in today’s world you need to do more than just comply with regulations to stay ahead of evolving threats. Health organizations are increasingly being targeted by cybercriminals. And with trends such as the Internet of Things, BYOD, and virtual healthcare, you need to protect your data and infrastructure across more fronts than ever. We help health organizations do that with our HIPAA BAA, trusted cloud services, and built-in security capabilities that work together across a comprehensive, agile platform to help enable end-to-end

Dartmouth-Hitchcock Medical Center is ushering in a new age of proactive, personalized healthcare with ImagineCare. It’s a cloud-based system that helps nurses and health coaches track and respond to an individual’s health status in real time.

Each patient’s personal care plan is continually updated in the secure, HIPAA-compliant system, using Cortana Intelligence Suite to evolve based not only on the person’s own data from Microsoft Dynamics CRM but also on near-real-time data from similar people, based on location, age, disease, biometrics, and more.

“We want to look at the whole population, because that’s what we’re accountable for, but we’re going to do it one individual at a time, because we want each patient to have the best possible experience,” says Dr. Robert Greene, Executive Vice President and Chief Population Health Management Officer at Dartmouth-Hitchcock.

To learn more about how Dartmouth-Hitchcock is harnessing transformative technologies to revolutionize healthcare, watch the video.
2. **A STRONG HISTORY OF COLLABORATION**

When you use Microsoft HIPAA BAA–covered cloud services, you benefit from our deep experience and health industry collaboration.

We’ve been executing HIPAA BAAs with customers since 2011. To create our HIPAA BAA, we collaborated with some of the leading U.S. medical schools and their HIPAA privacy counsel, as well as other public- and private-sector HIPAA-covered entities. Duke University, Emory University, Thomas Jefferson University, University of Iowa, and University of Washington chose Office 365 after the consortium of technology, legal, and compliance experts worked closely with us to develop our HIPAA BAA.

3. **MOST HIPAA BAA-COVERED CLOUD SERVICES**

Whether you need to better engage patients, empower care teams, optimize clinical and operational effectiveness, or transform the care continuum, you can choose from our wide range of cloud solutions to help you achieve your goals.

*Your compliance, your way – Microsoft HIPAA BAA*
To support our customers’ digital transformation needs, we offer more HIPAA BAA–covered services than any other cloud vendor. They include Microsoft Office 365, Microsoft Dynamics CRM Online, Microsoft Power BI, Microsoft Azure services, and Microsoft Intune. And we’re always adding more, so keep checking the list of services covered at: https://www.microsoft.com/en-us/TrustCenter/Compliance/HIPAA

Rather than piecing together cloud solutions from different vendors for productivity and collaboration, patient relationship management, analytics, application hosting, data storage, app and device management, and more, you can use our cloud services under one umbrella HIPAA BAA. That way, you can get the transformative technologies you require and a streamlined process to help you enable compliance across multiple solutions.

Learn how our cloud customers are empowering better health by viewing the customer story links throughout this paper and by visiting www.microsoft.com/health.

“It’s a seamless technology solution. That’s what makes ImagineCare possible—Cortana Intelligence Suite, Dynamics CRM, and Azure enabling big-data integration, predictive analytics, and machine learning on a seamless cloud-based platform. It’s allowing us to make a big difference in people’s lives.”

—Nathan Larson, Director of Remote Medical Sensing at Dartmouth-Hitchcock Medical Center

Read the case study >

4. STREAMLINED, SELF-SERVICE PROCESSES

We’re continually streamlining our BAA processes to make things simpler for health organizations. For example, customers who need to enter into a HIPAA BAA and who have an online service subscription agreement with Microsoft do not need to take any action to obtain or sign a HIPAA BAA because Microsoft automatically offers a HIPAA BAA to all such customers in the Online Services Terms.

And with the Service Trust Portal (STP), you can conveniently access a deep set of security, privacy, and compliance resources, such as independent audit reports of Microsoft cloud services, risk assessments, security best practices, and more. These include:

• SOC 1 and SOC 2 auditor’s reports.
• International Organization for Standardization (ISO) 27001 and 27018 audit reports and scope statements.
• Office 365 Information Security Management System (ISMS) guidance.
• Governance, risk management, security assessment, and compliance white papers, FAQs, and other materials to help you perform your own risk assessment.
What’s more, you can adjust the level of reporting to meet your needs. You can choose your industry and regional settings (which you can change at any time) so the STP can provide content relevant to your organization.

5. FLEXIBILITY TO IMPLEMENT SECURITY YOUR WAY

Your health organization has flexibility with our HIPAA BAA to design your security strategies your way. For example, unlike other cloud services vendors who offer a BAA, you’re not limited to just one way of encrypting data. Ask your IT team or partners about this and they’ll tell you that it’s much more efficient and effective for them to have the flexibility to design encryption the way they think is best for your organization, rather than being forced into one specific encryption methodology.

With our HIPAA BAA-covered services, you have many encryption capabilities and options at different levels of control. If you’d like to learn more, check out these helpful articles: Azure Data Security and Encryption Best Practices and Overview of Advanced Security Management in Office 365

Encryption options - overview

6. OPERATIONALIZED COMPLIANCE

We’ve instituted ongoing processes to stay up to date on meeting the latest technical, administrative, and physical safeguards as prescribed by HIPAA for cloud services covered under our BAA. In other words, we’ve operationalized compliance.

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 example, Microsoft Azure core services are audited by independent, external auditors under industry standards, including ISO 27001. Our ISO 27001 audit scope includes controls that address HIPAA security practices as recommended by the U.S. Department of Health and Human Services.

The ISO 27001 audit is an example of our ongoing compliance processes—it’s conducted at least twice a year.
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.

Toward that end, we offer several resources that you can reference to learn more about HIPAA security requirements and steps your health organization can take to help maintain compliance at: https://www.microsoft.com/en-us/TrustCenter/Compliance/HIPAA/

7. CLOUD PRINCIPLES OF TRUST
Beyond offering a HIPAA BAA, we also earn our customers trust by building our cloud services based on four core principles: control, privacy, security, and transparency.

We’re committed to helping you keep your data secure, private, and under your control. Microsoft cloud services can assist you in staying compliant, even as regulations and standards evolve. We’re also committed to being transparent about our security, privacy, and compliance practices. We understand the importance of knowing how your data is stored, accessed, and secured, and that you can independently verify this. Anytime there’s an issue, such as a security threat or a request by a government or law enforcement agency for access to customer data, we’ll keep you informed.

We’re also committed to reliability and choice. That is, our software and services must be robust to ensure you can access your data and services when you need to, and we need to give you the final say in decisions that impact compliance—such as having your data reside in your geographic region, and even in your own datacenter.

The Wellmark Blue Cross and Blue Shield Finder Service app lets members manage their healthcare experience from their mobile phones, tablets, and computers. To help partners build mobile and web apps that utilize this service, Wellmark needed to publish a Finder Service API. It turned to Microsoft Azure API Management. By choosing Azure API Management, Wellmark can provide partners with access to fresher, more precise data, reduce the risk and costs of API sharing, and make it easier for members to find providers.

“Our APIs, and by extension our member data, are better protected with Azure API Management, which helps us better meet HIPAA and other regulations.”

—Brad Hoyt, Director of Innovation and Emerging Technology at Wellmark Blue Cross and Blue Shield

Read the case study >

8. END-TO-END PROTECTION FOR TODAY’S WORLD
Your health organization is likely realizing that security isn’t just about complying with regulations such as HIPAA. And it isn’t just about your cloud services. Weakness anywhere in your technology stack can undermine security applied to other areas.
To avoid technology breaches and cyberattacks—which are so often in the news these days—you need to take an end-to-end approach to protecting your data and infrastructure. You need an approach that helps you answer questions like:

- **Are the people accessing your network who they say they are, and if they are, do they make preventable mistakes?**
- **Are the devices connecting to your network free from viruses and malware? What if they get compromised by a zero-day attack? What if they get lost or stolen?**
- **Can you trust the operating system and the software that runs on it to be robust and secure?**
- **Can you trust not only that your data is protected, but also that you know where it came from and it hasn’t been tampered with?**

Most cybercriminal schemes are successful because authentication controls and activity auditing around people, machines, software, and data are lacking.

We manage our cloud infrastructure across all these areas. When you put your infrastructure in our cloud, we manage the systems and software you use, and help protect your data with strong security controls and sound processes that are independently verified. And we have a portfolio of technologies that can help you prevent and mitigate breaches in areas you manage: the identities of your people, their devices, and the software and data on their devices.

For example, with **Windows 10**, you can take advantage of new ways to protect against today’s enterprise security threats such as hardware-based security for better malware protection and elimination; corporate identity security; data protection; more secure per-app connection for mobile workers; and more.

And with the **Microsoft Enterprise Mobility Suite**, you can manage mobile devices—whether personal or company-issued—to help ensure compliance whenever those devices are used to access company resources.

You can also help protect against unknown malware, viruses, and other sophisticated cyberattacks such as ransomware by applying behavioral analysis with **Exchange Advanced Threat Protection (ATP)**.

These are just a few examples. We build security into Microsoft products and services from the start. That’s how we deliver a comprehensive, agile platform to help you better protect your endpoints, move faster to detect threats, and respond to security breaches.

If you’d like to learn more about our latest end-to-end protection capabilities, check out:

- **Windows 10 for enterprise**
- **Azure security center**
- **O365 Security Blog**
- **Why Enterprise Mobility Suite**
- **Windows 10 Security**
9. INVESTING HEAVILY IN YOUR SECURITY

We invest more than $1 billion in security research and development each year. In November we announced new initiatives and investments in security that will help us better protect and secure our customers. We’ve created a dedicated group of worldwide security experts, the Microsoft Enterprise Cybersecurity Group, to deliver solutions, expertise, and services for Microsoft customers. We’ve also opened a Cyber Defense Operations Center that works 24×7 to protect against, detect, and respond to threats in real time. We bring together data points from billions of sources to give us unique insights into the threat landscape, and we apply those insights in our mission to help safeguard our customers’ privacy and their personal data.

Read a February 2016 progress report on enterprise security for our mobile-first, cloud-first world by our chief information security officer.

And stay up to date on our security efforts by visiting: www.microsoft.com/en-us/security

10. COMMITTED TO YOUR COMPLIANCE

In addition to our HIPAA BAA, our security investments have translated into dozens of industry certifications for our cloud platforms. Microsoft has a comprehensive set of certifications and attestations of any cloud service provider and we meet a number of health-specific compliance and certification agreements around the world, including the EU Model Clause. Learn more at: www.microsoft.com/en-us/TrustCenter/Compliance/default.aspx

“From a corporate compliance perspective, it is highly important that our patient data is protected and that only authenticated users can view it. Windows Azure Multi-Factor Authentication helps us do that.”

—Mike Baran, System Director, Technology, Presence Health

Read the case study
NEXT STEPS

You can find more information, videos, and specific guidance on implementing solutions that comply with the HIPAA and HITECH Act by visiting:

https://www.microsoft.com/en-us/TrustCenter/Compliance/HIPAA

Learn more about how you can empower better health with Microsoft products and services at http://www.microsoft.com/health.