HIPAA/HITECH Act Implementation Guidance for Microsoft Office 365 and Microsoft Dynamics CRM Online

HIPAA[1] and the HITECH Act[2] are U.S. laws that govern the security and privacy of personally identifiable health information stored or processed electronically. This information is referred to as electronic protected health information (ePHI). HIPAA refers to healthcare providers, payors and clearing houses that use or process ePHI as covered entities. Under HIPAA and the HITECH Act, covered entities must implement mandated physical, technical and administrative safeguards to protect ePHI. Certain service providers that store or process ePHI on behalf of covered entities are called business associates. Covered entities must ensure that their business associates implement similar security and privacy safeguards. For a covered healthcare company to use a service like Microsoft Office 365 or Microsoft Dynamics CRM Online, where ePHI would be stored or processed, the service provider will be a business associate and must agree in writing to implement required safeguards set out in HIPAA and the HITECH Act. This written agreement is known as a business associate agreement (BAA).

This guide was developed to assist customers who are interested in HIPAA and the HITECH Act in understanding the relevant capabilities of Microsoft Office 365 and Microsoft Dynamics CRM Online. The intended audience for this guide includes HIPAA administrators, legal staff, privacy officers, and others in organizations responsible for compliance with HIPAA and the HITECH Act, and implementation of physical, technical and administrative safeguards for protection of ePHI.

Although Microsoft Office 365 and Microsoft Dynamics CRM can help enable compliance, the ultimate responsibility for using our service and end -to-end compliance with HIPAA and the HITECH Act remains with the covered entity.

[1] The Health Insurance Portability and Accountability Act of 1996.

[2] The Health Information Technology for Economic and Clinical Health Act.

Sections below include:

- Microsoft Office 365 and Microsoft Dynamics CRM Online Services for Consideration
- Responsibilities of the Covered Entity
- Business Associate Agreements
- Evaluating Service Security and Applying it to a Compliance Program
- Understanding ePHI on the Service
- Procedures for Administrative Access
- Handling Security Breaches
- Checklist: Five Things to Do
- Additional Information

Microsoft Office 365 and Microsoft Dynamics CRM Online Services for Consideration

HIPAA support is currently built into and offered for the following services ONLY:
Office 365 Services as defined in the HIPAA Business Associate Agreement.
Microsoft Dynamics CRM Online sold through (i) Volume Licensing Programs, and (ii) the Dynamics CRM Online Portal.

Responsibilities of the Covered Entity

It is possible to use Microsoft Office 365 and Microsoft Dynamics CRM Online in a way that complies with HIPAA and HITECH Act requirements. However, customers are responsible for their own end-to-end compliance, as Microsoft does not analyze the contents of its customers' data, including what ePHI Microsoft processes.

This means each customer should have its own processes and policies in place to ensure its personnel do not use Microsoft Office 365 and Microsoft Dynamics CRM Online in a way that violates HIPAA and HITECH Act requirements.

For example, a HIPAA covered entity may store a patient's ePHI on a Microsoft service in a HIPAA-compliant manner. But if a doctor at that covered entity sends the ePHI through

Exchange Online to a marketer without the patient's permission, the covered entity may violate HIPAA.

The subsequent sections are designed to assist you in using the service appropriately, minimizing the risk of non-compliance with HIPAA.

Business Associate Agreements

To help comply with HIPAA and the HITECH Act, customers may enter into written agreements with Microsoft called business associate agreements or BAAs. Microsoft does not require customers to sign BAAs. Instead, Microsoft makes a HIPAA BAA available automatically to all customers with an online service contract in the Online Services Terms.

Customers with a BAA should designate appropriate individuals as Privacy Readers so they have access to the appropriate messages within Message center. You must refer to section **(ii) Contact Information for Notices** of the BAA for details on how to do this. If you do not do this, Microsoft may be unable to contact you for purposes as described in the BAA (e.g., to notify you in the event of a security breach involving ePHI).

Prior to placing ePHI in the online service, you should read this guide and the BAA in full and evaluate for yourself whether the BAA meets your needs and whether you should place ePHI in Microsoft Office 365 and Microsoft Dynamics CRM Online. Again, it is ultimately your responsibility to evaluate whether our services match the requirements of your HIPAA implementation strategy, and to ensure your personnel use these services in a way that complies with HIPAA requirements.

Evaluating Service Security and Applying it to a Compliance Program

Many of the Microsoft Office 365 and Microsoft Dynamics CRM Online offerings are certified under ISO 27001 by independent auditors. The scope of our ISO 27001 audits includes HIPAA security practices as recommended by the U.S. Department of Health and Human Services. To find out more about certifications for a particular service, you may consult the Microsoft Office 365 Trust Center and Microsoft Dynamics CRM Online Trust Center.

Note: The following offerings do not currently meet all recommended security requirements. It is strongly recommended that customers not place ePHI on these offerings:

- Microsoft CRM Dynamics Online administered through means other than the Office 365 Portal.
- Microsoft Dynamics CRM for supported devices (i.e. access through smartphones and tablets).

It is ultimately the customer's responsibility to determine the level of security that is appropriate for its requirements. A few specifics that you may wish to evaluate in your consideration of our security practices include the following:

- Encryption at rest and in-transit: Microsoft applies encryption-in-transit to transfer of information outside of Microsoft facilities. Encryption -in-transit only applies to information that can be encrypted without interfering with standard internet protocols. This means packet headers and message headers are not encrypted in transit, since that would interfere with delivery of the information. It is stronger recommended that you train and instruct your personnel to follow industry standard HIPAA security guidance to never put ePHI in the "from", "to", or "subject line" of an email message.

- Two Factor Authentication: Two-factor authentication is not available for customer authentication. Most services employ two -factor authentication for Microsoft's IT Operations team. If you wish to verify two -factor authentication practices on a particular service, you may contact Support to inquire about that service as described below.

- Security Configuration: Many services have optional security configurations that allow customers to change security parameters. HIPAA covered entities may wish to set such parameters at their highest security levels. For additional information on managing your ePHI to enhanced security, you will want to read the section below on the best ways to configure and use Microsoft Office 365 and Microsoft Dynamics CRM Online.

You may also reference the *Information Security Policy* or the *Standard Response to Request for Information – Security and Privacy* to assist in determining whether the offered services

are suitable for your use (current trial or paid customers only; prospective customers may inquire through Office 365 Support regarding reviewing this document).

If you have a question about whether a specific security requirement is met for any service, you may contact Microsoft Support. Microsoft will make commercially reasonable efforts to provide the information requested unless providing information at the requested level of specificity would degrade service security.

Microsoft Office 365 Support is located here.
Microsoft Dynamics CRM Online Support is located here.

Understanding ePHI on the Service

Microsoft processes enterprise customer data subject to detailed processes and controls for security, including ISO 27001 controls. Only certain data sets, however, are designated with the appropriate level of security and privacy to comply with the HIPAA security requirements, as described above.

Microsoft strongly recommends that you train your personnel to input ePHI only into the appropriately secured and designated areas.

The following data-sets or repositories are suitable for uploading ePHI:

- Email body
- Email attachment body
- SharePoint site content
- Information in the body of a SharePoint file
- Lync presentation file body
- IM or voice conversations
- CRM entity records

Examples of data-sets or repositories not suitable for inclusion of ePHI:

Examples Include

- Email headers, including “From”, “To”*, or “Subject Line”

- Filenames (including filenames of any attachments or uploaded documents on any Service)
- URLs, or any public SharePoint websites
- Account, billing, or service configuration data
- Internet domain names (e.g., "*fabrikam.com*")
- User global address list or address book data (including user account holder's name, user name, contact information and address book data)**
- Support ticket information (information sent directly from customer to support for troubleshooting, or information you request be accessed for Microsoft technical support)

* Since it is required for delivery, no email service, cloud or otherwise, will encrypt the "to, cc, bcc, or subject" lines of an email to a patient. This information will be available in-transit to multiple organizations. Your organization needs to evaluate on its own whether sending an email to a patient reveals ePHI, where the rest of the message is not ePHI or is encrypted.
** This means the service is likely unsuitable for your organization if you need to give user accounts to patients themselves. For example, the services may not be appropriate for a long-term care facility wishing to give its patients their own Exchange Online email accounts.

Procedures for Administrative Access

One of the ways that Office 365 and Microsoft Dynamics CRM Online assist you in controlling access to ePHI is by tracking each instance of access to data stored in the data sets or repositories identified as suitable for ePHI above. This includes access by Microsoft personnel, partners, or your own administrators. These access reports are available to the covered entity's administrators on request.

Microsoft recommends you regularly review these access reports to validate that only approved/appropriate individuals have accessed ePHI. For example, individuals designated as administrators have technical ability to access the mailbox of personnel in their organization. If a covered entity has established policies around when an IT administrator can enter into a doctor's mailbox, this report may assist you to verify that these polices are being followed.

Instructions on how to obtain these access reports for different services on Office 365 and Microsoft Dynamics CRM Online are available as on the following web-page in the Trust Center: http://www.microsoft.com/online/legal/v2/?docid=24

Handling Security Breaches

Upon becoming aware of a security breach involving ePHI, Microsoft will report this to all global administrators on the accounts and to any individuals assigned the Privacy Reader role. In addition, because Microsoft does not scan or otherwise interpret customers' data stored in the services, Microsoft will likely be aware only that a repository appropriate for storage of ePHI has been compromised. The customer will need to determine whether ePHI was actually present in the data set subject to a security breach.

Microsoft will report information it has developed on ePHI involved in a security breach within 30 days of the breach. Microsoft relies on the customer to handle all notifications to affected individuals.

Customers *should* assign appropriate individuals into the Message center Privacy Reader role. Global administrators and users assigned the Privacy Reader role will be able to view privacy or security notifications in Message center. In the event of a security breach, notifications will be posted to Message center, but the ability to see the detailed content of such posts is restricted to global admins or individuals who have been assigned the Privacy Reader role.

Customers may update their Privacy Reader admins at any time in Message Center.

Prior to sending a notification, Microsoft will work to contain the breach, analyze its impact, and assess the results. Depending on the nature of the breach, Microsoft may (a) provide customers a preliminary notification followed by subsequent details, or (b) wait until a full review has occurred and notify customers then. In either case, as stated above, Microsoft will notify customers within 30 days.

Checklist: Five Things to Do

- ✓ **Evaluate:** Make sure our security and privacy practices meet your requirements.
  - ✓ **Sign-Up:**
    - Review the BAA.
    - Designate your Privacy Readers in Message Center
- ✓ **Access Control:**

- Turn on Exchange Administrator Access Tracking, to know when your administrators have accessed user accounts. (instructions)
- Turn off Microsoft Dynamics CRM Online for supported devices. (instructions)
- Periodically request and review access control reports for data repositories in which you store ePHI **Training:**
  - Administrator Training: Train your administrators not to put ePHI in address book, directory, or global address list information, nor provide or allow access to ePHI during support services or troubleshooting with Microsoft. o User Training: Train your users not to put ePHI in email headers, filenames, or public SharePoint sites. Make sure users understand not to email ePHI to individuals who do not have the right to view that ePHI.

✓ **Establish Procedures:**

- Access Control: Make sure to review who has accessed user accounts, changed account passwords, or added themselves to shared resources.
- Privacy Contact: As your personnel change, make sure you update your Privacy Reader contacts.

Additional Information

The following information is not HIPAA -specific, but may assist you in understanding security and privacy in the services more generally to help you plan your HIPAA implementation strategy.

- Microsoft Office 365 Trust Center
- Microsoft Dynamics CRM Online Trust Center
- Microsoft HIPAA White Paper
- Microsoft Office 365 Security Whitepaper
- Microsoft Office 365 Standard Response Paper – Cloud Security Alliance Registry
- Microsoft Trustworthy Computing Data Governance Resources

Disclaimer

This guide is not intended to constitute legal advice. Customers should consult with their own legal counsel regarding compliance with HIPAA, HITECH Act, and other laws and regulations

applicable to their particular industry and intended use of Microsoft Office 365, Microsoft Dynamics CRM Online, and other Microsoft products and services. *Microsoft makes no warranties, express, implied, or statutory, as to the information in this document.*