# Cloud Computing Toolkit

## Acceptable Use Policy Template for Cloud Computing[1]

By the Cloud Computing Work Group

## Why Does my Healthcare Organization Need an Acceptable Use Policy for Cloud Computing?

Cloud computing services, such as those that offer Software as a Service (e.g. cloud-based email, online calendars, online word processors, etc.) or provide cloud-based storage of documents and other data, have become an increasing compliance and risk management challenge for healthcare organizations. For example, in 2015 the U.S. Department of Health and Human Services (HHS) entered into a $218,400 resolution agreement with a healthcare provider over the provider's workforce members' unauthorized use of an Internet-based document sharing application to store electronic protected health information (ePHI).[2]

## How to Use This Template

An Acceptable Use Policy ("Policy") provides guidance to employees and other workforce members (singularly referred to as "User" and collectively referred to as "Users") regarding the appropriate use of a healthcare organization's information technology resources and data (including ePHI and other confidential or sensitive information). For example, it may address the extent to which an enterprise-owned workstation or device may be used for personal use (e.g., use of social media for personal reasons). It may also address whether a User may install or deploy software on an enterprise-owned workstation or device (i.e., equipment owned by the healthcare organization).

The following is intended to provide a sample policy that healthcare organizations can insert (with appropriate modifications) into their main acceptable use policy to address the permissible and impermissible use of cloud computing services.

A healthcare organization can consider whether to implement technical safeguards such as monitoring or blocking the use of certain websites or services to help enforce this Policy. For example, cloud computing services which are not permitted may be blocked or otherwise monitored for enforcement purposes.

---

[1] This Acceptable Use Policy for Cloud Computing is intended to be a template to help your organization craft a cloud computing acceptable use policy. Also, it may be used as an "insert" to your organization's general acceptable use policy governing the appropriate use of information technology resources.

[2] Please see, *e.g.*, HHS, HIPAA Settlement Highlights Importance of Safeguards When Using Internet Applications (July 10, 2015), http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/SEMC/bulletin.pdf.

## Sample Policy Language

### Cloud Computing Services Acceptable Use Policy of [Healthcare Organization]

*Last revised*: _____

*Last adopted*: _____

---

## x.x Acceptable Use of Cloud Computing Services

### x.x.x Permitted Cloud-Based Applications for Use with Electronic Protected Health Information

Users are permitted to create, receive, transmit, or maintain electronic protected health information (ePHI) only on the following cloud-based applications. This must be done through an enterprise account of the [healthcare organization], rather than by setting up a personal account. An enterprise account may be established by [insert process for obtaining an enterprise account]. This Policy applies to both Users who are on-premises or working remotely [including working from home].

- [Cloud-Based Application Name], [Description], [Contact for obtaining enterprise account]
- [Cloud-Based Application Name], [Description], [Contact for obtaining enterprise account]
- [Cloud-Based Application Name], [Description], [Contact for obtaining enterprise account]

[Healthcare organization] has a business associate agreement in place with the above cloud-based application providers. Users may not create, receive, transmit, or maintain electronic protected health information on any other cloud-based applications, as doing so may violate HIPAA and other laws.

### x.x.x Permitted Cloud-Based Applications for Other Confidential or Sensitive Information

Users are permitted to create, receive, maintain, or transmit other confidential or sensitive information of the [healthcare organization], on the following cloud-based applications. Please see [insert name of policy which defines different types of information within the healthcare organization] for more information on what constitutes confidential or sensitive information. Confidential and sensitive information may only be created, transmitted, received, or maintained using an enterprise account, rather than a personal account. An enterprise account may be established by [insert process for obtaining an enterprise account].

[The healthcare organization may wish to ensure that this subsection addresses not only confidential information of the organization, but also sensitive information such as personally identifiable information (i.e., employees, workforce members, patients, and others), intellectual property (such as relating to patentable inventions, trade secrets, and copyrighted works), and confidential know-how of the organization.]

- [Cloud-Based Application Name], [Description], [Contact for obtaining enterprise account]

- [Cloud-Based Application Name], [Description], [Contact for obtaining enterprise account]
- [Cloud-Based Application Name], [Description], [Contact for obtaining enterprise account]

Users may not create, receive, transmit, or maintain confidential or sensitive information on any other cloud-based applications.

[Optional: Notwithstanding the foregoing, the following categories of confidential or sensitive information may not be created, received, transmitted, or maintained using cloud-based applications: _____.]

x.x.x Permitted Cloud-Based Communications Tools [E.g. E-mail, Video Conferencing, Instant Messaging]

Only the following cloud-based communications tools are permitted to help Users to conduct business or clinical duties of the [healthcare organization] using an enterprise account:

- [Cloud-Based Communication Tool Name], [Description], [Contact for obtaining enterprise account]

x.x.x Personal Use of Cloud-Based Applications and Cloud-Based Communication Tools

Users [may/may not] create, receive, maintain, or transmit information or other data for personal use on the enterprise accounts of any of the foregoing cloud-based applications, which have been authorized for use in accordance with this Policy.

Users [may/may not] use enterprise accounts of any of the foregoing cloud-based communication tools for personal use.

x.x.x Impermissible Use of Cloud-Based Applications

Users may not use other cloud-based applications to store [healthcare organization] documents or to conduct [healthcare organization] business or clinical duties. For example, Users may not create, receive, maintain, or transmit business or clinical documents using [list examples of cloud-based file sharing software that are not authorized]. Users may not conduct business or clinical duties through personal cloud-based e-mail accounts, such as [list examples of cloud-based e-mail services that are not permitted].

[If not already included in the acceptable use policy elsewhere] For questions about this Policy, contact: [insert contact name and contact information].

[If not already included in the acceptable use policy or other organizational policy, specify the consequences of violating the Policy.]