

July 27, 2012

Cloud Computing on the Internet

Guide for OHSU Faculty, Staff, Students, Departments, and Registered Organizations

GENERAL

The definition of cloud computing is complex, but for this guideline we will be using a definition that applies to individual user interaction with cloud services. Cloud computing services include applications and infrastructure that may allow the user extensive and mobile access to their information resources. A few examples of cloud computing for individuals are the Apple iCloud, Amazon Cloud Player, Google Docs, Dropbox, etc.

Because of the pervasiveness and use of these tools, security and regulatory concerns may arise, including:

- **Confidentiality:** most sites do not offer secure storage or transmission which means OHSU may lose the ability to keep certain information confidential. If we are required to keep the documents or information confidential by law (e.g., FERPA, HIPAA, etc) or pursuant to a contract, it exposes OHSU to monetary penalties and breach of contract claims.
- **Intellectual Property Rights:** many sites either expressly state that you lose ownership rights in data or information uploaded to the site or reserve the right to change their terms and conditions at any time. This exposes OHSU to loss of intellectual property rights in that data or information.
- **Data Accessibility:** sites may not provide access to the information if the site is shut down. This may affect compliance with our record retention policy or requirement to produce data when required by subpoena or government order, exposing OHSU to court imposed sanctions for failure to produce among other penalties.
- **Export Compliance:** many sites do not keep the information or data in the US. If controlled information or documents are stored in the site, it exposes OHSU- and whoever uploaded the information- to civil and criminal penalties.
- **HIPAA Compliance:** without having a business associate agreement in place with the cloud computing site we are in violation of HIPAA which exposes OHSU- and whoever uploaded the information- to civil and criminal penalties.
- **Lack of Control Over Data:** sites may be able to provide any documents or information stored on the site to governmental agencies without OHSU knowledge or ability to review or appeal the order or subpoena for the data.
- **Security Risks:** third party applications required by these sites expose OHSU to having viruses introduced into OHSU's network.

DATA STORAGE AND POSTING

Cloud services as described above are not permitted for University business purposes unless OHSU has a signed license agreement with the vendor, even if the contract offered is a click through agreement (where you just click accept online). All licensing agreements must be reviewed and approved by the OHSU Contracting Services Group prior to any use

of the service. Also note that there are usually business license agreements for such services; you may not accept a personal use license agreement if you are using the site for OHSU purposes or storing OHSU data, information or documents on the site.

You are **not** permitted to post OHSU confidential information, including any OHSU patient information, on any cloud services unless OHSU has signed a valid license agreement or you have received an exception to OHSU policy.

Examples of Confidential and Restricted Information:

- Any protected health information, including limited data sets
- Employee information
- Student information
- Financial information including budgets, marketing plans, invoices, contracts, etc.
- Proprietary Information including performance metrics, legal documents, etc.
- Classified or restricted research data
- Information OHSU is required by law or bound by contract to keep confidential

University Business Use

University Business Use can be defined as a department representing themselves as OHSU and making a business arrangement on behalf of OHSU using OHSU data or resources.

If OHSU has signed a valid license agreement with the specific cloud service provider, the use of that service should only be used for its intended purpose. Storage of data and use of the service for purposes other than its designated use may violate the license agreement could create regulatory issues (see General Section above).

Some cloud computing services are located in several different countries. **You** are responsible for ensuring that you do not put any information controlled by the U.S. Government on such sites and for compliance with U.S. Export Control laws.

Personal Use

Consistent with the OHSU Acceptable Use of Computing Policy, personal use of University electronic resources to access Cloud Computing Service sites is to be limited to incidental use. Incidental use must not interfere with an individual’s performance of his/her assigned job responsibilities or someone else’s job performance or compromise the functionality of the department or campus network.

If you use cloud computing services on your computer at OHSU, make sure you understand the license agreement before you agree to it. Individuals may be in violation of the license agreement if they use the service on a business network. Some cloud license agreements remove a user’s ownership rights to the data and/or permit the cloud services provider to use the data a user puts on the service for its own business purposes.

RISKS – SPAM, SPYWARE, AND VIRUSES

Cloud computing services may require the user to download and install an application that interfaces with the resource. From time to time, these applications may need to be updated to mitigate a vulnerability in the software. Because older versions of software increase the risk of virus exposure, and because it is required by OHSU policy ([ISD-700-00019](#)), users of this software must implement updates when available.

Sharing data through the cloud can also allow the user to access and retrieve documents that may be infected with viruses or other malware. Users should not share their cloud computing resources with individuals they do not know or trust and should NEVER share their password to these resources with individuals they do not know or trust.

MONITORING

Any information you post on the internet is public information. You are responsible for knowing how to use cloud computing services, managing any information you share on such sites, and for being compliant with all University and applicable website policies as well as applicable laws and regulations.

Since information posted on the Internet is public, Oregon Health & Science University may monitor cloud computing sites and, as with other electronic resources, University systems administrators may perform activities necessary to ensure the integrity, functionality, and security of the University's electronic resources.

QUESTIONS:

If you have any questions regarding the classification of OHSU data please contact the OHSU Office of Information Privacy and Security at 4-8849.

RELATED RESOURCES

Acceptable Use of Computing and Telecommunications Resources #11-20-010

<https://o2.ohsu.edu/policies-and-compliance/ohsu-policy-manual/chapter-11-information-technology/ohsu-policy-11-20-010.cfm>)

Confidentiality #01-05-010

<https://o2.ohsu.edu/policies-and-compliance/ohsu-policy-manual/chapter-1-administration/ohsu-policy-01-05-010.cfm>)

Confidentiality of Health Information #01-05-012

<https://o2.ohsu.edu/policies-and-compliance/ohsu-policy-manual/chapter-1-administration/ohsu-policy-01-05-012.cfm>)

Export Compliance #01-05-006

<https://o2.ohsu.edu/policies-and-compliance/ohsu-policy-manual/chapter-1-administration/ohsu-policy-01-05-006.cfm>)

Student Records - Confidential Records - Restrictions on Release #02-20-025

<https://o2.ohsu.edu/policies-and-compliance/ohsu-policy-manual/chapter-2-student-affairs/ohsu-policy-02-20-025.cfm>)

Secure Storage of Electronic Restricted Information

<http://ozone.ohsu.edu/cc/sec/isp/00006.pdf>)

Secure Transmission of Electronic Restricted Information

<http://ozone.ohsu.edu/cc/sec/isp/00007.pdf>)

End-User Applications

<http://ozone.ohsu.edu/cc/sec/isp/00018.pdf>)

Use of OHSU Name; Endorsements; Sponsorships #08-10-009

http://ozone.ohsu.edu/policy/pac/chapt_8/8-10-009.htm)

Code of Conduct

<http://www.ohsu.edu/xd/about/services/integrity/policies/upload/2011OHSU-Code-of-Conduct.pdf>

OHSU Strategic Plan: Vision 2020

http://www.ohsu.edu/xd/about/vision/upload/OHSU_Vision_2020_strategies.pdf

User Agreements for Electronic Resources (see providers' Web sites)
