Title: Cloud Computing: Opportunities Used Safely
Number: G4-004D
Responsible Office: Information Security and Privacy Office
Last Revision: June 2019

The following guidance was developed and published by the University of Pennsylvania. Minor modifications have been made to reflect the policy and environment of the University of Utah. Attachments B, C, and D were added in their entirety. The full citation for the article can be found in the end-notes.[i]

GUIDANCE

This guidance is to describe opportunities, issues, safeguards and requirements regarding the use of certain third-party services (often called "cloud computing" services) involving University data. While there are many uses of the phrase "cloud computing," in general, it refers to free or low cost services offered worldwide to any individual user where resources, such as infrastructure or software, are provided over the Internet. In many cases, data resides on the cloud provider's servers.

The developments in cloud computing in recent years are providing new opportunities for many faculty and staff at The University of Utah to communicate, collaborate, and compute more effectively to serve The University of Utah's mission. For example, social networking sites may be appealing as interactive course communication tools, and as platforms to support formation of constituent groups. Faculty and staff may sometimes wish to use third-party online data storage to house teaching, research and administrative data. A variety of collaboration tools also exist "in the cloud" that can facilitate research and related endeavors involving colleagues at the University and all over the globe. These online services, which are often free or low-cost, can seem very inviting. Usually, individuals are prompted to sign up for such services under a "click through" (i.e., non-negotiable) agreement and pay only for the resources they directly use. However, there are compliance and other risks when University data is shared outside of the University. This guidance is intended to explain those risks, given the existing technology. As the technology changes, which it will, we will update this advice accordingly.

1. Each faculty, staff member, and/or department and staff member considering a cloud computing service should consider the following issues before sharing[ii] University of Utah data with a cloud computing service:
    a. Sharing University data with a company that is new and may go out of business is high risk, particularly if there is no backup at the University. Important work could be lost forever.
    b. Sharing sensitive, private information about individuals could present significant privacy and security risks if the cloud service provider is not providing assurances of strong privacy and security practices.
    c. Some cloud providers store data in other countries—this could present a problem of foreign government access to data of interest and also could pose export controls problems (again, consider the nature of the work being performed).
    d. See a fuller list of issues in Attachment A. It is important to consider the type of project and type of data involved in working through the issues list in Attachment A. For example, when sensitive personal data or critical business data to support University operations are involved, one should be very cautious and ensure that proper controls exist to address the concerns raised in the Attachment.

2. It is unlawful to share certain types of data with a cloud provider—or any third party—unless there is an agreement that properly reflects legal requirements. For example, data privacy protections provided by HIPAA, by FERPA , and often by funding agencies require specific language in agreements with third parties handling regulated data. At this point, most "terms of service" that cloud providers ask users to "click through" to agree upon, do not contain such language. Faculty and staff must not utilize cloud providers to handle HIPAA, FERPA or other regulated data unless the terms of service contain the required language (Business Associate Agreement) or unless there is a negotiated agreement to ensure compliance. The Information Security and Privacy Office or the Office of General Counsel should be consulted where any questions arise in this area.

3. Special Note Regarding E-Mail. In cases where individuals have two active e-mail accounts—a University account and a separate account with a third-party provider such as Gmail or Hotmail—the University account alone should be utilized whenever practicable when dealing with the information described above. In cases where an individual uses the University account only for automatic forwarding to a third-party e-mail provider, faculty and staff should take special care not to include information described above in e-mail, unless a negotiated agreement governs the third-party e-mail account or the terms of service contain required language for compliance.

4. There is a legal requirement that where University data is shared with a third party, the faculty or staff member sharing such data must be able to retrieve it when asked. At times, the University must ask faculty and staff to provide certain data for legal, investigatory and compliance reasons. Sometimes that means individuals must bring work papers to campus from home; sometimes IT staff must retrieve data from backups.

Similarly, where faculty and staff are storing University data with third-party online services, they must be prepared to access and provide such data should a legal, investigatory, or compliance reason arise. Therefore, it is impermissible for faculty and staff to utilize a third-party service where they will lose the ability to access and retrieve the University data they share with that service.

In short, faculty and staff considering sharing certain data with any third-party services have a responsibility to review and follow this guidance. Where such sharing is permissible, faculty and staff should also review the terms and conditions of using such services to make sure that the issues highlighted in this Guidance, including Attachment A, are properly addressed. If there is any doubt about the proposed agreement please consult the Office of General Counsel.

Attachment A

For data that can be shared with a third party, consider the following issues before utilizing third-party "cloud" services.

There may be instances where University faculty, staff members, post-docs or others wish to utilize third-party services for data relating to research, scholarly or other purposes. If the data at issue is not regulated by privacy or security laws, such services may be appropriate. However, consider the following issues:

- *Continued availability of data.* Certain services are more reliable than others and some may be able to demonstrate their reliability. Consider this and the consequences of a service becoming unavailable or a company going out of business. In such cases, would you be able to gain access to the data you entrusted to the service? Would your business continuity needs be met?

- *Ownership of data.* Each service has its own terms and conditions of use. Some terms and conditions may assert that the service can exercise rights over data in its possession, now or in the future. Also, services often reserve the right to change their terms and conditions without notice. Consider whether unencumbered data ownership rights (for example, intellectual property rights) are important with respect to your data.

- *Security of the information.* Some services may utilize adequate technical safeguards, physical access controls and limitations on disclosure; others may not. These are important factors to keep in mind if you wish to protect your information from unintended disclosure. A third-party certification such as a TRUSTe seal or a European Union Safe Harbor certification can provide some added comfort that a security review has been conducted.

- *Privacy controls.* If the service involves data-sharing activities, the user may wish to limit data access in certain ways. Determine whether the service provides an easy and reliable way to limit data sharing in accordance with your wishes.

- *Contractual/Funding Obligations.* The program may have agreed to certain data protection terms in a contract, or via the requirements of a funding agency or other organization. Review any agreements to ensure that sending of data to the third party is permissible.

- *Jurisdictional issues.* Different legal requirements may be triggered by different data locations. For example, Amazon provides data storage services located physically in the US and Europe, and allows users to keep their data in whichever they choose. Where data resides can have important legal implications in terms of (1) whose law applies and (2) the likelihood of foreign government access to the data.

- *Export Controls.* A related issue lies in the area of export controls. If you are working with export-controlled information or software, the computing environment you are working with becomes very important. You may unwittingly be "exporting" certain information without a license where one may be required. Those unsure of whether information or software is subject to export limitations should consult the University's Export Controls resources at *xxx.*

- *Support.* Consider the potential consequences of using a service whose support level may be unknown. You may need support services to, for example, address difficulties in using a particular application, conduct a search involving large volumes of data, or retrieve data for use by colleagues in the event of your inability to do so (for example, during a hospital stay).

- *Monitoring*. Monitoring is a key component of the assurance process and provides information on adherence to any service level agreements that may be in force.

- *Legal*. It is crucial that your legal counsel be involved in the process in drafting any agreement with a cloud provider. (See Attachment D).

  The following controls are recommended when entering into any agreement with a cloud provider.

Note: Internal resources may meet your computing needs without taking on the risks that exist "in the cloud." Please visit https://uofu.service-now.com/it?id=uofu_portal for more information on available options.

Attachment B

Entities that are covered by the Health Insurance Portability and Accountability Act ("HIPAA") are required to ensure the confidentiality of protected health information ("PHI"). In general terms, PHI includes all health information that is personally identifiable. As with education records, PHI may not be shared or stored with third parties unless an appropriate contractual agreement is in place to protect the data. It is worth noting, in addition, that the recent economic stimulus legislation greatly increased the penalties associated with HIPAA violations.

The Family Educational Rights and Privacy Act ("FERPA") requires that education records be protected from inappropriate disclosure, as defined by the Act. Under FERPA, education records include all records that are directly related to a student, and maintained by the University. Examples include student grades and student assignments that are handed in. Education records may not be shared or stored with third parties (including online services) unless the party is under the University's contractual control regarding the use and maintenance of the records.

Note also that a University constituent using the University logo online or elsewhere is responsible for assuring that the logo is used appropriately.

Attachment C

On April 21, 2011, a large cloud provider experienced a major outage and took down a number of large commercial web sites. The outage lasted for two days and occurred when a configuration error occurred in a data center located in the US.

It appears that due to a network glitch, a number of storage volumes created duplicate backups and filled the cloud provider's ready capacity. The major selling point of this provider was elasticity which provides for rapid

and automatic infrastructure scale up during periods of increased traffic spikes. The same elasticity is repeated when the spikes fall off and the system contracts and the expanded capacity is no longer needed.

The point of caution being that no matter the strength of the agreement between the provider and a customer, when the system goes down, the customer must recognize that the provider may be unable to fulfill aspects of the contract and damage could occur to the customer.

Attachment D

The following items should be considered when you are evaluating legal/contractual language:

1. Will the contract specify the specific infrastructure and security controls, obligations, and practices (business continuity, encryption, firewalls, physical security, etc.)? The required controls included in the contract should include those listed in the Control Survey (worksheet 3a, 3b, or 3c, according to System Risk Score).
2. Will the contract include a right-to-audit clause? Does the service provider have a Type II SSAE 16, SOC 2, SOC 3, or other audit or attestation report? If yes, please provide a copy of the report.
3. Will the Service Level Agreement (SLA) specify uptime requirements? What are the uptime requirements?
4. Will the contract include a description of the functionality of services being provided?
5. Will the contract specify any third-parties the service provider relies on for provisioning the service? Please list them.
6. Will the SLA specify performance and response time requirements? What are they?
7. Will the SLA specify error correction time requirements? What are they?
8. Will the contract specify that the University retains all ownership rights to the data?
9. Will the contract specify that the University retains the right to access and retrieve University content in the event of contract termination? Is a timeframe for providing access specified?
10. Will the contract guarantee confidentiality of University data, even after contract termination?
11. Will the contract require that the service provider report to the University any data breach associated with the service or University data?
12. Will the contract specify the location of University data? What location(s) is (are) specified?

[i] Beck, Robin and Mary Lee Brown. Cloud Computing: Opportunities Used Safely. 03 Mar. 2010. University of Pennsylvania Almanac March 30, 2010 Volume 56 No. 27. 1 May 2011 <http://www.upenn.edu/almanac/volumes/v56/n27/cloud.html>.

[ii] "Sharing" as used in this guidance means to provide data that is in plain text, or which the third-party online service has the capability to decrypt.