THE HARVARD CLINICAL
AND TRANSLATIONAL
SCIENCE CENTER

Information Risks & IRB Strategies for Technologies Used in Research: A Guide for Researchers, IT, and IRBs

Last updated: September 25, 2016

Table of Contents

1.	**Overview**	Pg.3
2.	**Data Classification**	Pgs. 4-5
3.	**Technologies**	Pgs. 6-31
3a.	**Live Two-Way Communication**	Pgs. 6-10
3b.	**Physical Storage**	Pgs. 11-15
3c.	**Mobile Devices and Applications (Apps)**	Pgs. 16-21
3d.	**Survey Tools**	Pgs. 22-26
3e.	**Cloud Service and Storage**	Pgs. 27-31
4.	**Additional Resources**	Pgs. 32-39
4a.	**Investigator Checklist for Securing Research Data**	Pgs. 32-33
4b.	**Guidance on When to Encrypt Data**	Pg. 34
4c.	**Points to Consider When Choosing a Cloud Service**	Pgs. 35-36
4d.	**Glossary of Common Terms for Technologies Used in Research**	Pgs. 37-39
5.	**Attribution, Sharing, and Adapting**	Pg.43
6.	**Acknowledgements and Contact Us**	Pg.44
7.	**Bibliography**	Pgs.45-50

1. Overview

The use of technologically interconnected products and services continues to revolutionize the design and conduct of research as researchers can now more easily find, recruit, and communicate with subjects, as well as select cohorts from larger candidate pools, and may do so with greater precision. New tools enable electronic data capture through surveys and devices that collect, analyze, and store a multitude of biological and environmental measures.

These technological innovations raise important legal, regulatory, and ethical questions for researchers and institutional review boards (IRB) alike. Among them, do IRBs and researchers understand how information is collected, used, and stored in sufficient detail to protect human research subjects? Can IRBs and researchers assure patients that uses of technology conform to promises or assurances made during the informed consent process? At stake are research subjects' privacy, confidentiality, and trust in the medical research enterprise.

IRBs and researchers need to fully understand how new technologies work to enable reasonable assessments of risks to research data and implementation of data protection safeguards to eliminate, mitigate, or reduce these risks. While the IRB and Information Technology (IT) work together to understand the safety and potential risks of the technology, ultimately the principal investigator (PI) is the responsible party. Ideally the PI should be working with IT during project planning so that the safety and potential risks of the technology are known and can be shared with the IRB at the time of IRB submission.

This Guide to Technologies Used in Research offers a primer on broad categories of technologies used in research along with a list of issues to consider when assessing data security risk. The additional resources section includes materials to further assist researchers, IT, and IRBs by providing supplementary steps to protect research data.

If you wish to request, share, adapt, or contribute to this document, please see the 5. Attribution, Sharing, and Adapting section.

Finally, we would like to thank all those who contributed to the information gathering, drafting, and editing of this document. To learn more about those who contributed, please see our 6. Acknowledgments and Contact Us section at the end of the document.

2. Data Classification

While IT and IRBs assess information risk, they often do so from diverse perspectives and regulatory mandates. IT staff, for example, are often trained in frameworks designed for large enterprise systems or for financial transaction integrity. Examples include Federal Information Security Modernization Act (FISMA), Federal Information Processing Standards (FIPS), International Organization for Standardization or ISO 27001, Payment Card Industry Data Security Standard (PCI-DSS), and others. IRBs, however, assess information risk in light of federal regulatory mandates designed to protect human research subjects. These include the Federal Policy for the Protection of Human Subjects, also known as the 'Common Rule', and regulations enforced by HHS Office of Human Research Protections (e.g., 45 CFR 46, et seq.); the HIPAA Privacy Rule and Security Rule (45 CFR 160 and 164 et seq.); Food and Drug Administration (FDA) regulations; as well as assorted state laws. The task of information risk assessment is further complicated by ongoing innovations in research design, and the continually changing nature of the content, format, and rules of access for data sources that are accessed electronically.

A response to these differing perspectives and mandates for assessing information risks has been for institutions to develop data classification policies that characterize data sensitivity and risk along a spectrum of confidentiality, identifiability, and other factors justifying tiered levels of administrative, physical, and technical safeguards.

Data classification is one of many policy responses an institution may employ to assess risk to research data held by an institution or its researchers. As regulatory authorities continue to emphasize applying and documenting risk assessments, institutions handling sensitive research data may want to document their consideration of data classification policies as part of an overall risk assessment system for both research subject protection purposes and for compliance with other data security frameworks.

Key areas for consideration and questions to ask during risk assessment:

1. **Data Ownership:** Who owns the data? Any given piece of technology is subject to data ownership conflicts questioning who owns data, including pre-existing data sets or data produced by research. For example, technology used in research may automatically transfer ownership interests without the authorization of the individual, institution, or researcher. A relevant to question ask is: Does a third party vendor automatically collect data in the cloud without authorization by the researcher or research subject?

2. **Data Collection:** How does a given technology collect data? Researchers should only collect information that is needed. Technology should be checked to ensure that only the intended data are being collected. Investigators are responsible for working with IT to determine what kind of data the technology is collecting and how to best protect that data. Some services require the data to be extracted from the data source and transported into a data warehouse, also know as, *Extract, Transform, Load (ETL)* process. While in some studies a person will manually enter data, in others, smart phones may automatically collect the user's geo-location data that may then be used in research. Each of these methods presents risks that must be understood and mitigated.

3. **Data Access:** How is existing data analyzed, processed, or viewed? Data may be held on a device or in the 'cloud' but viewed through a smart phone or desktop computer. How is access

managed? Are there access controls? Are individuals given the minimum necessary access required to perform a given research task?

4. **Data Storage:** How is the data kept or held? Is the data being stored on a server, handheld device, or drive, or by a third party vendor? The method of data storage can affect the risk that the data will be lost, stolen, or viewed by unauthorized parties. For example, data held on a server with an open port connected to the internet may be exposed to public search engines.

5. **Data Transmission:** Data transmission refers to data in motion from one machine or device to another. Research data may be transmitted in a variety of ways such as over wired or wireless networks, using various transmission technologies such as internet protocols, cellular phone protocols, or public switches and routers.

6. **Data Sharing:** Data sharing may involve the research collaborator/co-PI or staff who share data with other members of the study team. In other cases, data sharing may involve moving large data sets to make them available to others outside the study team for research purposes. Risks associated with data sharing may involve unauthorized use, disclosures, etc. These risks may be reduced through management and monitoring of proper user controls. Examples of risk assessment considerations for data sharing include:

    - ☑ Technologies may enable multiple people to view, edit, or analyze data in a shared research space. Consider ways to control data viewing such as remote locking, timed-out locking, password protections, etc.
    - ☑ Note whether there are, or will be, external collaborators. Identify external collaborators and note if the technology has the capability to verify access, how access will be monitored, and which data and subsets of data require access by external collaborators.
    - ☑ Ensure whenever possible that the data has been de-identified.
    - ☑ If applicable, ensure appropriate local policy is in place (e.g., data use agreement, terms of use, etc.).
    - ☑ If applicable, ensure the technology establishes a secure web-based portal.

7. **Data Retention and Destruction**: If data needs to be stored for long periods of time, the technology chosen to store the data should be assessed to ensure long-term access for personnel monitoring and support for the form of media. The technology should be periodically reviewed to determine if the data needs to be moved to an updated storage option (e.g., moving data from a CD-ROM to a USB). Data that is no longer needed in a research study should be destroyed. A proper disposal policy may include ensuring that sensitive information is shredded, and that media holding sensitive information is cleaned according to industry standards once that information is no longer needed for the research.

Encryption is the conversion of data into a format that is not easily understood by unauthorized viewers. Encryption can be applied to storage devices (data "at rest") and to network data (data "in transit"). The type of computing device and network, and whether personal or Protected Health Information (PHI) is involved, will dictate whether encryption is required. Encryption is a great way to protect your research data but it is not required if you do not store or work with research data that includes personal information or PHI. For more information on when to encrypt data, see the Guidance on When to Encrypt Data, in the 4. Additional Resources section.

3. Technologies

Researchers use both institutional and non-institutional tools and technology to conduct research. IT reviews technology to help navigate the researcher to the best media for the research study. IT vets the technology to minimize the risks for the research participant and comply with regulations. IRBs review protocols using vetted and non-vetted technology (technology that hasn't been reviewed and approved by IT). This section describes several types of technologies used in research and each technology's related risk considerations and possible mitigation strategies.

3a. Live Two-Way Communication

What is live two-way communication technology?

Two-way communication technology enables simultaneous communication between two or more individuals through audio and visual communication channels. Commonly used forms of live two-way communication technology include telephone, instant messaging (e.g., text messaging, Google Hangout, etc.), chat rooms (e.g., Yahoo Chat), and video telephony or internet phone (e.g., FaceTime, Skype, WebEx, using web cameras, etc.). Instant messaging is a communication tool that allows users to send typed messages, pictures, files, and live video to one or more recipients. Chat rooms are similar to instant messaging but instead of one-to-one communication, users log into a virtual room or space to communicate with others in the "room".[1] Video telephony or internet phone is a real-time, audio-visual communication tool. Live two-way communication technologies use telecommunication networks established through public switch-enabled telephone wires, cellular networks, and other analog and digital technologies.

Prior to submitting an IRB application or amendment for research studies using live two-way communication technology, the following risks and technology considerations should be addressed:

The confidentiality, integrity, and availability of data collected using live two-way communication technologies may be susceptible to threats. Information risks associated with live two-way communication technologies can arise when the technology is susceptible to wiretapping or interception of data, or when the technology or website keeps track of a user's activities. Unless data is encrypted and access controls are in place, anyone with physical access to a local area network (LAN) could potentially connect monitoring tools and access the communications occurring across that network. Technologies that rely on wi-fi are vulnerable if not protected by updated Wi-Fi Protected Access (WPA) using Advanced Encryption Standards (AES)[2].

Important risks associated with live two-way communication technologies:

1. **Data Ownership:** Live two-way communication providers may impose terms of service that are buried in fine print. These terms of service may unintentionally grant third parties access or intellectual property rights to data in violation of the communicating parties' expectations and data protection obligations.

[1] http://www.familysafecomputers.org/imchat.htm, 01/23/2016
[2] [2] See NIST 800-111

2. **Data Collection:** Communication providers may use software that automatically collects data from users. Technology vendors may, by default, set live two-way communication technologies to collect data not intended or necessary to collect for the research.
3. **Data Access:** If the live two-way communication provider records communications or collects metadata (e.g., time, location, address, etc.), then depending on the company's policies, you may not have a right to access the information the company has collected.
4. **Data Storage:** The chosen communication technology, such as a smartphone, may be enabled to store or record live two-way communications. This presents a risk of unauthorized disclosure if the phone is lost or compromised. As a result, a research team may need to add additional technology and protections to enable such recordings or data storage.
5. **Data Transmission:** Live two-way communication technology may transmit data in a variety of forms over wired or wireless networks, using various transmission technologies such as internet protocols, cellular phone protocols, or public switches and routers. Depending on the circumstances, these channels may not be encrypted or secure. The technology software may be vulnerable if not regularly updated and patched. Whenever possible, don't transfer files via email; instead use an encrypted USB or external drive. When using email, never use your personal email account, as it is not secure. Make sure your work email is set up to be secure. To ensure the security of data being transmission, you can type in the subject line "[send secure]" in front of the subject title. Never include PHI in the subject title; subject titles are not secure.
6. **Data Sharing:** Files and images can be shared through live two-way communication technologies. Data sharing is accomplished over telephone wires, wi-fi, Bluetooth, and other data transmission technologies. Depending on the circumstances, these channels may not be encrypted or secure. The technology software may be vulnerable if not regularly updated and patched.
7. **Data Retention/Destruction:** Vendors of live two-way communication technologies may deny users the ability to retain or destroy data collected by the company. Users should address this in contractual terms if possible.

To **eliminate, mitigate and/or reduce risk,** investigators can communicate with IT, research computing, or information security to ensure that network infrastructures used for the research study have in place appropriate physical safeguards, access controls (collect and access only the minimum necessary information to conduct the study), and encryption.

A researcher can take steps to ensure data protection and privacy by managing policies, supporting role-based controls, and having IT and research compliance review research plans. Researchers should share with their institutional IT or research computing resource any contracts or agreements they have with data providers affecting rights, roles, and responsibilities pertaining to the data. Each user has the ability to control some collaboration parameters through use of the role-based controls (i.e. granting login credentials). IT can grant privileges based on the user's affiliations and role in the research study. IT can use granular control to grant access to specific services and data based on roles, groups, or the needs of a particular user.

Live two-way communication vendors may offer IT the ability to manage collaboration privileges and to enforce enterprise security policies. A policy, contract, or agreement may include prohibiting automatic recording or disclosures of identifiable information to third parties without authorization.

Appendix: Considerations to eliminate, mitigate, or reduce risks related to the use of *live two-way communication technologies* in research

A. When developing research study design and methods, describe procedures and safeguards for:

Collecting and recording research data:

- ❑ Explain your selection criteria for the technology in the research protocol.
- ❑ Provide detailed information about what the technology does and its role in the study. Include information about the technology manufacturer, if applicable, such as a brochure, screen shots, version dates, or other information for reviewers.
- ❑ Specify whether a participant's personal device or a device provided by the research study will be used.
- ❑ Explain whether the tool/technology will be password-protected.
- ❑ Describe the method of data collection and how often the data will be collected. Specify whether the data will be transmitted to a server behind your institution's firewall or to another site.
- ❑ Explain how the participant will be informed that the data is subject to the technology's terms of agreement, and told how the terms may change over time.

Processing, coding, and maintaining access to research data:

- ❑ Specify where and under which conditions individuals will have access to the data (what will be made available and to whom).
- ❑ List all parties, including IT, that will have access to the data. Make sure this list is always up to date.
- ❑ If outside collaborators will be granted access, explain how this will be done. List the information they will have access to and any agreements you have in place.
- ❑ Specify whether participants will be given a research code number to protect their identity when using this technology.

Storage of research data:

- ❑ Specify where the data will be stored and who will have access to it. Data should be kept in a secure location, a place only the PI and authorized research staff can access (both electronically and physically).
- ❑ Indicate how the data will be protected.
- ❑ Remove necessary subject identifiers from data files, and encrypt data files if stored electronically. Identifiers should be stored in a physically separate and secure location from the data files, and associated with the data files through a key code that is also stored in a separate and secure location. Additional justification must be provided to rationalize retention of subject identifiers to meet the specific needs of the research study.
- ❑ Specify whether the data will be stored or transmitted immediately. If not transmitted immediately, explain.

Sharing and transferring research data:

- ❑ Fully describe any third-party involvement, including their access to and/or retention of the data and their plans for use or reuse. Make sure to include in the informed consent document.

- ❑ Specify which data is transmitted to a server, and indicate if that exchange is encrypted. See the *Guidance on When to Encrypt Data.*
- ❑ Indicate which secure modes of transmission of data will be used (e.g., VPN, secure file transfer, etc.).
- ❑ Data submitted electronically and/or subject identifiers submitted over a public network must be encrypted.
- ❑ Consult with IT if there will be any external collaborators.

Research data destruction and minimizing potential risks to subject's confidentiality:

- ❑ Explain where the data will go when the study is over (e.g., deleted from the shared folders, de-identified and stored for future use, etc.).
- ❑ If the data will be destroyed, explain how this will be done and by whom, and provide an estimated timeline.
- ❑ Specify at what point subject identifiable data will be de-identified or destroyed.

B. Consult with IT to review the technology, institutional policies, and any required agreements:

Begin communicating with IT early in the process, as they will need to conduct their own review of the technology. This can sometimes include working with the technology provider on use agreements.

Review the technology and account:

- ❑ Review your institution's policy on security controls and safeguarding data. Determine whether data can be loaded onto other storage devices such as servers, disks, or portable media. Ensure secure transmission of data within an institution, and review how data saved on the institutional server should be properly deleted.
- ❑ Conduct a risk assessment on the technology. Review the chosen technology and determine if another technology would better fit the research study objectives.
- ❑ Determine the electronic and physical storage methods. Specify how data will be stored or transmitted.
- ❑ Review needs for encryption. Ensure appropriate encryption is in place (e.g., mail, internet, etc.). Determine plan(s) to prevent interception of data by a third party. See the *Guidance on When to Encrypt Data*.
- ❑ If there will be external collaborators, identify them and determine if the technology has the capability to verify access. Specify how access will be monitored and identify which data and subsets of data require research access.

Review the servicer and account:

- ❑ Review and verify the security standards of the servicer.
- ❑ Determine who owns the data and how much data will be stored. Determine if the servicer charges by the amount of data. Determine if there are additional costs to protect data.
- ❑ Determine whether the servicer will destroy the data or re-write the data and at what point the data will be destroyed.
- ❑ Determine whether the servicer will return the data, and if yes, how this is done.
- ❑ Determine whether the server is stored outside the US, and whether the information is subject to international or export restrictions.

Consult with appropriate individuals and/or offices, which may include IT and legal, to determine if the technology will require a Business Associate Agreement (BAA): The majority of services require that you sign their terms and conditions prior to using the service. When possible, try to negotiate a contract with the servicer.

- ❑ Review the policy to understand how your research might be affected if another company buys the service provider. Determine if the sale would affect the data ownership, disaster recovery, privacy policies, or other issues.
- ❑ The terms of services should address:
  - ❑ Privacy rules and regulations
  - ❑ Safety of non-public information (SSN, credit card information, etc.)
  - ❑ Value of intellectual property
  - ❑ Any grant funding requirements regarding security, human subjects privacy regulations, or confidentiality.
- ❑ If applicable, address who reviewed the BAA, and who will continue to review updates of the agreement.

3b. Physical Storage

What is physical storage technology?

A media or any tangible material (portable media) used to store data, including but not limited to tapes (e.g., reel, cassette), flash drive (e.g., USB), magnetic disk storage, cartridges, disks, drums, CDs, DVDs etc. Ensure the conditions under which the information is stored protect against inappropriate interaction with or inadvertent interception of participant information.[3] Research records should be maintained at the office, laboratory, or department where they were created or used, or on an electronic computing system maintained by the institution, preferably behind a firewall.[4]

Prior to submitting an IRB application or amendment for research studies using physical storage technology, the following risks and technology considerations should be addressed:

Information risks associated with physical storage media can arise because the technology can be used over a wireless network, making the communication susceptible to wiretapping or interception of data. The most common threats are hackers, computer criminals, terrorists, industrial espionage, and/or disgruntled employees.[5] Natural disasters such as floods, earthquakes, and/or tornados leave the data vulnerable to loss or exposure to unauthorized parties. Many institutions have policies in place regarding selecting physical storage; check with your IT Department about your institution policy.

Important risks associated with physical storage technologies:

1. **Data Ownership:** Research data collected and stored on physical storage media is typically owned and/or governed by the investigator's institution or by the sponsor of the research. Therefore, personal data of the PI or research staff should not be stored on or intermingled with institutional or work computer systems.
2. **Data Collection:** Physical storage media collects data manually or uses software (e.g., cookies and web beacons) to automatically collect data from users. During data collection, there is a risk of data failing to correctly save to the media or of data access records inadvertently being deleted, which will make the most current version of the data unavailable.
3. **Data Access:** Data may be accessed in different locations depending on the physical storage media and the platform through which it is accessed. If the physical storage media is accessed remotely, additional precautions should be in place to protect the information (e.g., password protected login, ability to logoff users after a set time, ability to lock access if password is entered incorrectly over a set amount of times, etc.). In some cases, users may opt in or opt out of services but by doing this, may sacrifice access to services and data. If opting into physical storage services, choose only the minimum services necessary, and limit the number of staff who can access the media. Physical storage media may allow for password protected access and remote locking capabilities.
4. **Data Storage:** Data should be stored on the appropriate media specified to protect the sensitivity of the data, with appropriate access requirements. Access rights should be defined for all folders and files in the physical storage media (e.g., only select research staff have the authority to modify backup files). Remove necessary subject identifiers from data files, and encrypt data files if stored electronically. Identifiers should be stored in a physically separate

[3] http://humansubjects.stanford.edu/hrpp/Chapter11.html

[4] http://vpr.harvard.edu/search/site/storage%20media

[5] http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/nist800-30.pdf

and secure location from the data files, and associated with the data files through a key code that is also stored in a separate and secure location. There is also the risk of more information being stored than is necessary. Data stored on physical devices (e.g., smart phones, hard drives, physical servers, etc.) present the risk of unauthorized hacking, copying, loss, theft, or other dissemination that violates data use and protection terms. Server ports should be actively monitored and secured as they pose a disclosure risk through the exposure on internet search engines (e.g., Google, Yahoo, etc.).

5. **Data Transmission:** Data is transmitted when the physical storage media is connected to a device designed to read the media. For example, data stored on a USB is transmitted when the USB is plugged into a device equipped with the necessary plugin to read the data. Risks include access by unauthorized users, mishandling of data, and failure to remove the device from the media when no longer in use. Whenever possible, don't transfer files via email; instead use an encrypted USB or external drive. When using email, never use your personal email account, as it is not secure. Make sure your work email is set up to be secure. To ensure the security of data being transmission, you can type in the subject line "[send secure]" in front of the subject title. Never include PHI in the subject title; subject titles are not secure.
6. **Data Sharing:** Files and images can be stored, shared, and saved through physical storage media. Data sharing is accomplished over telephone wires, wi-fi, Bluetooth and other data transmission technologies. Depending on the circumstances, these channels may not be encrypted or secure. The technology software may be vulnerable if not regularly updated and patched.
7. **Data Retention/Destruction:** The duration of time the data will be stored on the physical storage media should be taken into account when determining the risks. Special file deletion software can be used to overwrite data, making data recovery impossible. Additionally, the media should be reviewed to determine if reading is possible while the data is being stored. This is especially critical for long-term storage or archiving. Account for the fact that storage media products can have varied shelf lives, and may become obsolete (data can become unreadable to current technology, such as zip drives, or degrade with storage time, as with CDs and DVDs).

To **eliminate, mitigate and/or reduce risk,** investigators can communicate with IT, research computing, or information security to ensure that network infrastructures used for the research study have in place appropriate physical safeguards, access controls (collect and access only the minimum necessary information to conduct the study), and encryption.

To mitigate the risk of mishandling private information, investigators and IRBs must consider the risks associated with physical and digital storage, and evaluate and implement methods to reduce these risks.

A researcher can take steps to ensure data protection and privacy by sharing with institutional IT and research compliance all of the written and oral agreements and understandings they have with respect to pre-existing research data and data intended for collection. Researchers should work collaboratively with IT and research computing groups to design infrastructure that protects the data and advances the research. For example, research IT may decide that portable devices or laptops should not persistently store sensitive research data but may access data via secure web portals.

IT should be consulted on how and when the data will be retained and destroyed once the physical storage media is no longer in use. Specify the timeframe for the use and storage of the data.

Appendix: Considerations to eliminate, mitigate, or reduce risk related to the use of *physical storage* technologies in research

A. When developing research study design and methods, describe procedures and safeguards for:

Collecting and recording research data:

- ❑ Explain your selection criteria for the physical storage technology in the research protocol.
- ❑ Provide detailed information about what the technology does and its role in the study. Include information about the technology manufacturer, if applicable, such as a brochure, screen shots, version dates, or other information for reviewers.
- ❑ Explain whether the physical storage technology will be password-protected.
- ❑ Describe the method of data collection and how often the data will be collected. Specify whether the data will be transmitted to a server behind your institution's firewall or another site.
- ❑ Provide confirmation that the research staff has signed a confidentiality agreement, agreeing to protect the security and confidentiality of identifiable information.

Processing, coding, and maintaining access to research data:

- ❑ Specify where and under which conditions individuals will have access to the data (what will be made available and to whom).
- ❑ List all parties, including IT, that will have access to the data. Make sure this list is always up to date.
- ❑ If outside collaborators will be granted access, explain how this will be done. List the information they will have access to and any agreements you have in place.
- ❑ Specify whether participants will be given a research code number to protect their identity when using this technology.

Storage of research data:

- ❑ Specify where the data will be stored and who will have access to it. Data should be kept in a secure location, a place only the PI and authorized research staff can access (both electronically and physically).
- ❑ Indicate how the data will be protected.
- ❑ Remove necessary subject identifiers from data files, and encrypt data files if stored electronically. Identifiers should be stored in a physically separate and secure location from the data files, and associated with the data files through a key code that is also stored in a separate and secure location. Additional justification must be provided to rationalize retention of subject identifiers to meet the specific needs of the research study.
- ❑ Specify whether the data will be stored or transmitted immediately. If not immediately, explain.

Sharing and transferring research data:

- ❑ Fully describe any third-party involvement (i.e. Amazon Cloud services or research service using a cloud service provider), including their access to and/or retention of the data, and their plans for use or reuse. Make sure to include in the informed consent document.
- ❑ Specify which data is transmitted to a server, and indicate if that exchange is encrypted. See the *Guidance on When to Encrypt Data*.

- ❑ Indicate which secure modes of transmission of data will be used (e.g., VPN, secure file transfer, etc.).
- ❑ Consult with IT if there will be any external collaborators.

Research data destruction and minimizing potential risks to subject's confidentiality:

- ❑ Explain where the data will go when the study is over (e.g., deleted from the shared folders, de-identified and stored for future use, etc.).
- ❑ If the data will be destroyed, explain how this will be done and by whom, and provide an estimated timeline.
- ❑ Specify at what point subject identifiable data will be de-identified or destroyed.

B. Consult with IT to review the technology, institutional policies, and any required agreements:

Begin communicating with IT early in the process, as they will need to conduct their own review of the technology. This can sometimes include working with the technology provider on use agreements.

Review the technology and account:

- ❑ Review your institution's policy on security controls and safeguarding data. Determine whether data can be loaded onto other storage devices such as servers, disks, or portable media. Ensure secure transmission of data within an institution, and review how data saved on the institutional server should be properly deleted.
- ❑ Conduct a risk assessment on the technology. Review the physical storage technology and determine if another technology would better fit the research study objectives.
- ❑ Determine the electronic and physical storage methods. Specify how will data be stored or transmitted.
- ❑ Review needs for encryption. Ensure appropriate encryption is in place (e.g., mail, internet, etc.). Determine plan(s) to prevent interception of data by a third party. See the *Guidance on When to Encrypt Data.*
- ❑ If there will be external collaborators, identify them and determine if the technology has the capability to verify access. Specify how access will be monitored and identify which data and subsets of data require research access.

Review the servicer and account:

- ❑ Review and verify the security standards of the physical storage technology.
- ❑ Determine who owns the data and how much data will be stored. Determine if the servicer charges by the amount of data. Determine if there are additional costs to protect data.
- ❑ Determine whether the servicer will destroy the data or re-write the data and at what point the data will be destroyed.
- ❑ Determine whether the servicer will return the data, and if yes, how this is done.
- ❑ Determine whether the server stored outside the US, and whether the information subject to international or export restrictions.
- ❑ Contact your IT office or Information Security Officer to ensure your physical storage technology choice is appropriate.
- ❑ Determine all physical devices that will store or transmit data.
- ❑ Check for your institutional policy on safeguarding data from unauthorized intrusion or natural disasters.

- ❑ Ensure your workstations are limited to authorized users only who have appropriate validation.
- ❑ Determine where paper-based records will be stored and who will be designated access to records.
- ❑ Research data access should be limited only to necessary research staff who are granted privileges and gain access to the data by password.

Consult with appropriate individuals and/or offices, which may include IT and legal, to determine if the technology will require a Business Associate Agreement (BAA): The majority of services require that you sign their terms and conditions prior to using the service. When possible, try to negotiate a contract with the servicer.

- ❑ Review the policy to understand how your research might be affected if another company buys the service provider. Determine if the sale would affect the data ownership, disaster recovery, privacy policies, or other issues.
- ❑ The terms of services should address:
    - ❑ Privacy rules and regulations
    - ❑ Safety of non-public information (SSN, credit card information, etc.)
    - ❑ Value of intellectual property
    - ❑ Any grant funding requirements regarding security, human subjects privacy regulations, or confidentiality.
- ❑ If applicable, address who reviewed the BAA, and who will continue to review updates of the agreement.

3c. Mobile Devices and Applications (Apps)

Mobile devices and applications or "apps" allow for remote subject monitoring and data collection. Through these technologies the access to data is improved while potentially lowering costs and time commitment burden on research subjects.

What is a mobile device?

A **mobile device,** (e.g., laptop, tablet, "smart" phones, portable storage media, etc.) is a handheld tablet or other device that is made for portability, intended for remotely accessing or processing data. If you plan to use a mobile device as a medical device, then you are requesting to use a **mobile medical device** (e.g., wireless home sleep apnea test, EKG, etc.). Transforming a mobile device into a regulated medical device is done by using attachments, sensors, or other peripheral device. [6]

What is an app?

An **app**, (e.g., fitness tracker, podcast channel, calendar), is a software application that is designed to perform a specific function. It can be run on a mobile platform, or a web-based software application.[7] Apps are designed to run on the operating system of the platform or software it is being accessed through until it is closed out or exited. In some cases, apps may remain running and collect data in the background. You are able to control how apps refresh their content when on wi-fi or cellular in the background. For example, iPhone apps can be updated in the Background App Refresh setting. Here you can close out apps and control when they update themselves. If you plan to use a mobile app as a medical device, then you are requesting to use a **mobile medical app.**

If you think the device or app may meet the definition of an FDA regulated device, contact the IRB early for a consultation. Detailed FDA guidance is available at the FDA Regulations and Guidance.8 For a complete list of what is classified as a mobile medical device or app, visit the FDA webpage.

Prior to submitting an IRB application or amendment for research studies using mobile device or app, the following risks and technology considerations should be addressed:

Mobile devices are a high-risk technology because they are more susceptible to loss and theft, unauthorized access, and use of unsecured wireless services. Information risks associated with mobile devices and apps can arise because the technology is often used with a wireless network, making the communication susceptible to wiretapping or interception of data. Risks associated with mobile devices and apps can be mitigated by using secured wireless networks (e.g., virtual private network (VPN), encrypted mobile devices ,malware software[9] The mobile device or app technology should be configured to only keep track of the users activities if it has been approved with the research study. Unless data is encrypted and access controls are in place, anyone with physical access to a local area network (LAN) could potentially connect monitoring tools and tap into the communications. Technologies that rely on wi-fi may be vulnerable to being compromise if not protected by updated Wi-Fi Protected Access (WPA) using Advanced Encryption Standards (AES)[10] [11](e.g., anti-malware, IDPS, DLP, etc.). Depending on the mobile technology, the device may allow remote locking or deletion of data.

[6] http://www.farmpd.com/Farm-Blog/bid/78079/Five-Promising-Medical-Device-Mobile-Apps 02/02/16
[7] https://kb.wisc.edu/hsirbs/page.php?id=41771
[8] FDA Regulations and Guidance
9 (Houlding "Healthcare Information at Risk")
[10] See FIPS Standard Publication 197
[11] See NIST 800-111

Important considerations for mobile device and app technology:

1. **Data Ownership**- Research data collected and stored on mobile device and app technology is susceptible to all or some of the data being owned by the developer. Data ownership is outlined in the terms of service for each technology. When a mobile device and app technology is "running" or "open", a variety of data is being collected without showing signs to the user. The technology should always be shut down or closed out after use so that no additional data can be collected. Researchers should clarify any data owned by the developer.
2. **Data Collection**- Mobile device and app technology may be set to automatically collect data by tracking cookies[12] and web beacons [13]. The technology vendor notifies the user of the automatic data collection in the terms of use, which must be accepted when the device is first used then periodically. Recording elements include: geo-location information, activity, length of calls, duration of internet connection, number of messages sent and received: Short Message Service (SMS) commonly known as "text message," Multimedia Messaging Service (MMS) is a text message that includes a photo, video, or audio (e.g., taking a photo with a camera phone and sending the photo to another device). Settings should be configured to restrict additional apps, or other data resources from being downloaded onto the device being used for research, protecting any risks that may incur.
3. **Data Access**- Data may be accessed in different locations depending on the mobile device and app technology and the platform through which it is accessed. Precautions should be in place to protect the device and the information: encrypt the device, password protected login (with a strong password typically six or more characters), "PIN" (personally identifiable number) login, ability to logoff users after a set time, ability to lock access or delete data if password is entered incorrectly over a set amount of times (typically this is set for three to ten attempts), remote locking capabilities, etc. Antiviral software and updates should be consistently checked to ensure the most recent safety precautions are applied to the technology. Failure to make updates in a timely manner increases the risk of data being mishandled. Access controls should be prior to use by the research participant.
4. **Data Storage**- Data that is stored on a mobile device or app technology should be encrypted, de-identified, or coded to protect the data. Mobile device and app technology allow for data storage in many locations, including on the device or a third party (e.g., cloud). Automatic backups of the devices should also be encrypted, either in the cloud or on a local PC.
5. **Data Transmission**- Mobile device and app technology transmit data through another mobile device, wireless network, or other data transmission technology. Risks include interception by an unauthorized user, mishandling of data, and failure to update and patch software to the latest models and anti-virus protection. Depending on the circumstances, these channels may not be encrypted or secure. Transfer sensitive data from the mobile device or app technology as soon as possible to reduce risk. To ensure data being transmitted is secure, you can type in the subject line "[send secure]" in front of the subject title to make the email secure. Never include PHI in the subject title, the subject title is not secure.

[12] A text file placed on user's computer by a website or web server. Often used to keep track of individuals as they navigate a site, and more broadly, the web. *Internet-Based Research-CPHS University of California, Berkley Cphs.berkeley.edu/internet_research.pdf*. Berkeley, CA: University of California, Berkeley, 07 July 2015. PDF.

[13] An embedded object in a web page or email, typically transparent that tracks behavior or use of the web page or email. Web beacons can be detected by looking for tags that load from a different server then the one being used. Often web beacons are embedded with cookies. Beal, Vangie. "Web Beacon." *What Is Web Beacon? Webopedia Definition*. Webopedia. Web. 06 Apr. 2016. <http://www.webopedia.com/TERM/W/Web_beacon.html>.

6. **Data Sharing**- Files and images can be stored, shared, and saved on the mobile device and app technology or a third party. Data sharing is accomplished over wi-fi, Bluetooth, docking or plugging in to a compatible device that can transmit the data. Depending on the circumstances, these channels may not be encrypted or secure. Research data should only be shared when the security of the recipient's systems is known and is satisfactory to the sensitivity of the data.
7. **Data Retention and Destruction-** The duration of time the data will be stored on the mobile device and app technology should be taken into account when determining the risks. Depending on the mobile device or app company, data retention and destruction policies with differ, including how the data will be retained and destroyed. Work with your IT and legal offices to determine if a Business Association Agreement (BAA) or other contract is needed. If a mobile device will be used by more than one research participant over the course of the study, plan for how and when data should be taken off the device prior to the next research participant's use of the device.

To **eliminate, mitigate, and/or reduce risk, i**nvestigators can communicate with IT, research computing, or information security to ensure that network infrastructures used for the research study have in place appropriate physical safeguards, access controls (collect and access only the minimum necessary information to conduct the study), and encryption. "In order to mitigate the risk associated with mobile devices and apps, it is important to know the differences in risks between personal use and mobile devices and apps used for research. Personal mobile devices are less manageable than corporate devices"[14]. If a personal mobile device, also called "Bring Your Own Device", or BYOD (e.g., smart phone, iPad, etc.), is used to capture or share information it must be secured appropriate to the sensitivity of the data. To reduce risk, a mobile device management, or MDM, infrastructure can be implemented to isolate the application from the rest of the mobile device and app operating system.

To mitigate the risk of mishandling private information, investigators and IRBs must consider the risks associated with mobile device and app technology, and evaluate and implement methods to reduce these risks.

A researcher can take steps to ensure data protection and privacy by sharing with institutional IT and research compliance all of the written and oral agreements and understandings they have with respect to pre-existing research data and data intended for collection. Researchers should work collaboratively with IT and research computing groups to design infrastructure that protects the data and advances the research. For example, research IT may decide on parameters through the use of role-based controls, granting privileges based on the user's affiliation and role in the research study. Remote access technology may be set up to delete or lock data in the event of theft or lose of the technology. Research data should never be stored on unencrypted devices as these devices are susceptible to loss or theft.

IT should be consulted on how and when the data will be retained and destroyed once the mobile device and app technology is no longer in use. Specify the timeframe for the use and storage of the data.

[14] (Houlding "Healthcare Information at Risk")

Appendix: Considerations to eliminate, mitigate, or reduce risk with *mobile device and apps technologies* in research

A. When developing research study design and methods, describe procedures and safeguards for:

Collecting and recording research data:

- ❑ Explain your selection criteria for the mobile device or app in the research protocol.
- ❑ Provide detailed information about what the mobile device or app does and its role in the study. Include information about the mobile device or app manufacturer, if applicable, such as a brochure, screen shots, version dates, or other information for reviewers.
- ❑ Specify whether a participant's personal device or a device provided by the research study will be used.
- ❑ Explain whether the mobile device/app technology will be password-protected.
- ❑ Describe the method of data collection (e.g., audio recording, fitness tracker, etc.) and how often the data will be collected. Specify whether the data will be transmitted to a server behind your institution's firewall or to another site.
- ❑ Explain how the participant will be informed that the data is subject to the technology's terms of agreement, and told how the terms may change over time.
- ❑ Specify if your study includes the use of a **mobile medical app**. If so, it may be subject to FDA regulations. Detailed FDA guidance is available at the FDA Regulations and Guidance. For a complete list of what is classified as a mobile medical device, visit the FDA webpage. It is recommended to consult with the IRB early in the research study design process.

Processing, coding, and maintaining access to research data:

- ❑ Specify where and under which conditions individuals will have access to the data (what will be made available and to whom).
- ❑ List all parties, including IT, that will have access to the data. Make sure this list is always up to date.
- ❑ If outside collaborators will be granted access, explain how this will be done. List the information they will have access to and any agreements you have in place.
- ❑ Specify whether participants will be given a research code number to protect their identity while using the mobile device or app.

Storage of research data:

- ❑ Specify where the data will be stored and who will have access to it. Data should be kept in a secure location, a place where only the PI and authorized research staff can access (both electronically and physically).
- ❑ Indicate how the data will be protected.
- ❑ Remove necessary subject identifiers from data files, and encrypt data files if stored electronically. Identifiers should be stored in a physically separate and secure location from the data files, and associated with the data files through a key code that is also stored in a separate and secure location. Additional justification must be provided to rationalize retention of subject identifiers to meet the specific needs of the research study.

- ❑ Specify whether the data will be stored or transmitted immediately. If not transmitted immediately, explain.

Sharing and transferring research data:

- ❑ Fully describe any third-party involvement by the mobile device or app developer, including their access to and/or retention of the data and their plans for use or reuse. Make sure to include in the informed consent document.
- ❑ Specify which data is transmitted to a server, and indicate if that exchange is encrypted. See the *Guidance on When to Encrypt Data*.
- ❑ Indicate which secure modes of transmission of data will be used (e.g., VPN, secure file transfer, etc.).
- ❑ If your funder is NIH or NSF, indicate how you have planned for their data-sharing requirements (e.g., The NIH advises that personally identifiable, sensitive, and confidential information about NIH-supported research or research participants not be housed on portable electronic devices).

Research data destruction and minimizing potential risks to subject's confidentiality:

- ❑ Explain where the data will go when the study is over (e.g., deleted from the shared folders, de-identified and stored for future use, etc.).
- ❑ If the data will be destroyed, explain how this will be done and by whom, and provide an estimated timeline.
- ❑ Specify at what point subject identifiable data will be de-identified or destroyed.

B. Consult with IT to review the technology, institutional policies, and any required agreements:

Begin communicating with IT early in the process, as they will need to conduct their own review of the technology. This can sometimes include working with the technology provider on use agreements.

Review the technology and account:

- ❑ Review your institution's policy on security controls and safeguarding data. Determine whether data can be loaded onto other storage devices such as servers, disks, or portable media. Ensure secure transmission of data within an institution, and review how data saved on the institutional server, should be properly deleted.
- ❑ List if automatic backup of the data will be implemented to either a server or PC.
- ❑ Conduct a risk assessment on the technology. Review the mobile device and app technology and determine if another technology would better fit the research study objectives.
- ❑ Determine the electronic and physical storage methods and how the data will be stored or transmitted.
- ❑ Review needs for encryption. Ensure appropriate encryption is in place (e.g., mail, internet, etc.). Determine plan(s) to prevent interception of data by a third party. See the *Guidance on When to Encrypt Data*.
- ❑ If there will be external collaborators, identify them and determine if the technology has the capability to verify access. Specify how access will be monitored and identify which data and subsets of data require research access.

Review the mobile device or app technology and account:

- ❑ Review and verify the security standards for the mobile device or app servicer.

- ❑ Determine who owns the data and how much data will be stored. Determine if the servicer charges by the amount of data and if there are additional costs to protect data.
- ❑ Determine whether the servicer will destroy the data or re-write the data and at what point the data will be destroyed.
- ❑ Determine whether the servicer will return the data. Explain how will this is be done.
- ❑ Determine whether the server is stored outside the US and whether the information subject to international or export restrictions.

Consult with appropriate individuals and/or offices, which may include IT and legal, to determine if the technology will require a Business Associate Agreement (BAA): The majority of services require that you sign their terms and conditions prior to using the service. When possible, try to negotiate a contract with the servicer.

- ❑ Review the policy to understand how your research might be affected if another company buys the service provider. Determine if the sale would affect the data ownership, disaster recovery, privacy policies, or other issues.
- ❑ The terms of services should address:
  - ❑ Privacy rules and regulations
  - ❑ Safety of non-public information (SSN, credit card information, etc.)
  - ❑ Value of intellectual property
  - ❑ Any grant funding requirements regarding security, human subjects privacy regulations or confidentiality.
- ❑ If applicable, address who reviewed the BAA and who will continue to review updates of the agreement.

3d. Survey Tools

What is survey tool technology?

A technology that enables the collection of data through a series of questions relevant to the audience invited to complete the survey. Researchers conduct survey research by using web-based survey tools (e.g., using the internet, a user can log-on to a site and fill out the survey), and externally hosted online surveys tools. The most common survey tools used for research include REDCap, Research Use, Qualtrics, LimeSurvey, and Survey Monkey.

Prior to submitting and IRB application or amendment for research studies using survey tools, the following risks and technology considerations should be addressed:

Information risks associated with some survey tools arise because the technology functions over a wireless network and through a third-party platform. The wireless network makes the data susceptible to wiretapping or interception of data. The technology or website may keep track of the user's activities. When determining the risks to subjects' privacy and confidentiality, the sensitivity of the data being collected must be considered. If an invasion of privacy or a breach of confidentiality would place subjects at risk of embarrassment or harm (including criminal or civil liability), or could be damaging to their financial standing, employability, insurability, reputation, or be stigmatizing, it may be unacceptable to collect sensitive data online via the internet without encryption or other methods that guarantee anonymity.[15] Consult with your IT Department if the survey tool technology will collect identifiable information (e.g., name, address, email, IP address, etc.).

Important risks associated with survey tool technology:

1. **Data Ownership**- According to their terms of service, survey tools may own some of the data and may also collect a variety of data that the company does not consider owned by the user. Companies often harvest sensitive data for advertising profiling.
2. **Data Collection**- Survey tools collect data manually or use software (e.g., cookies and web beacons) to automatically collect data from users. may be set to collect unintended data by the technology vendor. Depending on the survey design identifiable data may be collected (e.g., Intellectual Property (IP) addresses, email addresses, etc.) thus allowing survey sites to trace survey response data back to individual responders.
3. **Data Access**- Data may be accessed in different locations depending on the survey tool. If on a personal device, additional risks may be considered (e.g., the terms of agreement for the personal device were accepted under personal terms not considering the use for research). Access rights should be defined for all folders and files in the physical storage media (e.g., only select research staff have the authority to modify backup files). Remove necessary subject identifiers from data files, and encrypt data files if stored electronically. Identifiers should be stored in a physically separate and secure location from the data files, and associated with the data files through a key code that is also stored in a separate and secure location. There is also the risk of more information being stored than is necessary. Data stored on physical devices (e.g., smart phones, hard drives, physical servers, etc.) present the risk of unauthorized hacking, copying, loss, theft, or other dissemination that violates data use and protection terms. Server

[15] Partners Human Research Committee

ports should be actively monitored and secured as they pose a disclosure risk through the exposure on internet search engines (e.g., Google, Yahoo, etc.).

4. **Data Storage**- Data should be stored on the appropriate media specified to protect the sensitivity of the data, with appropriate role-based access. Data from a survey tool can be stored on survey software, on the platform used to access the survey, with a 3rd party (e.g., Cloud), or your institution's server. A research team may need to add additional technology and protections to enable the data storage.
5. **Data Transmission**- Data transmission refers to data in motion from the machine or device to another. Research data may be transmitted in a variety of ways such as export from survey software to secured file, over wireless network, etc. Depending on the survey tool, the risk level may increase based on the method used to transfer data (e.g., wireless transfer intercepted by unauthorized parties) and if the survey tool software is not up to date. Survey tools should be encrypted and protected by a strong password. If possible, also set-up a timed lockout of the survey tool after a set time of inactivity. When sending out a link to the survey, the risk levels increase with the possibility of interception of data through email and text channels.
6. **Data Sharing**- Survey data and analysis can be shared within the survey platform to authorized users, by requesting the platform to email the survey data and reports by sending the data or sending a link to the data, or by saving the data to your server. Access should be given through proper access controls such as: password protection, encrypted files, etc. Research data should be shared only when the security of the recipient's system is known and is appropriate for the sensitivity of the data. When possible, don't transfer files through email. Instead use an encrypted USB or external drive. When using email, never use your personal email account as it is not secured. Your work email should be set up to be secure. To ensure the email is secure you can type in the title box "[send secure]" to the front of the email title to make the email secure. Never include PHI in the subject title, the subject title is not secure.
7. **Data Retention and Destruction-** Depending on the survey tool authorized users will be given read, write, edit, or delete access. Make sure appropriate access is given based on the research staff members role and always transfer data when staff leave; removing their access completely. If data needs to be stored for a long period of time, the survey tool chosen should be assessed for long-term access for personnel monitoring and the form of media. Data that is no longer needed for a research study should be destroyed. A proper disposal may include removing the data from the survey tool, shared files servers, etc.

To **eliminate, mitigate and/or reduce risk,** investigators can communicate with IT, research computing or information security to ensure that network infrastructures used for the research study have in place the appropriate physical safeguards, access controls (collect and access only the minimum necessary information to conduct the study), and encryption. Internet-based research must meet the same criteria for IRB approval and offer the same level of protections to human research subjects as research conducted through more traditional methods. Consider whether the web-based survey tool affords adequate privacy and confidentiality protections and ensures that additional risks related to Internet research are minimized The IRB should work with IT to develop a list of vetted survey tools for researchers to use. When the IRB reviews the use of web-based survey tools, the IRB must specifically. In order to mitigate the risks associated with survey tools, it is important to understand the different risks associated with web-based and externally hosted survey tools. If a personal device is used to access the survey tool it must be secured in the same manner as an institutional device. Consult with IT to determine the ability to trace responses back to individuals via their e-mail address, their Intellectual Property (IP) address, or other identifying information captured while visiting the survey website.

A researcher can take steps to ensure data protection and privacy by managing policies, supporting role-based controls, and having IT and research compliance review research plans. Researchers should share with their institutional IT or research computing resource any contracts or agreements they have with data providers affecting rights, roles, and responsibilities pertaining to the data. Each user has the ability to control some collaboration parameters through use of the role-based controls (i.e. granting login credentials). IT can grant privileges based on the user's affiliations and role in the research study. IT can use granular control to grant access to specific services and data based on roles, groups, or the needs of a particular user.

Survey tool vendors may offer IT the ability to manage collaboration privileges and to enforce enterprise security policies. A policy, contract, or agreement may include prohibiting automatic recording or disclosures of identifiable information to third parties without authorization. Survey tool technology should be chosen based on the best option for the research study. Consider offering alternative methods of participating in the study if subjects prefer not to submit their information online.

Appendix: Considerations to eliminate, mitigate, or reduce risk related to the use of *survey tool technology* in research

A. When developing research study design and methods, describe procedures and safeguards for:

It is important to know how to create a survey to ensure compliance with the regulations associated with human subject protections. These include offering an alternative means to completing the survey, such as printing the survey or mailing it in, designing the survey so that participants can skip questions or decide not to answer, and providing the option to submit the data or discard the data, ensuring that a participant has the right to withdrawal at any point and have their data removed from the study.

Collecting and recording research data:

- ❑ Explain your selection criteria for the survey tool in the research protocol.
- ❑ Provide detailed information about what the survey tool does and its role in the study. Include information about the technology manufacturer, if applicable, such as a brochure, screen shots, version dates, or other information for reviewers.
- ❑ Explain whether or not the survey tool will be password protected. Indicate whether the survey is by invitation only, with a code (login/password) or available to the public.
- ❑ Specify whether a participant will be asked to use their own device to complete the survey or if a device provided by the research study will be used.
- ❑ Describe the method of data collection (e.g., email link to participants, post link to website, etc.) and how often the data will be collected (e.g., is this a one-time response survey). Consider the validity of data and the possibility of people completing surveys multiple times.
- ❑ Explain whether the data is transmitted to a server behind your institution's firewall or to another site.
- ❑ Explain how the participant will be informed that the data is subject to the survey tool's terms of agreement, and told how the terms may change over time.

Processing, coding, and maintaining access to research data:

- ❑ Specify where and under which conditions individuals will have access to the data, what will be made available, and to whom.
- ❑ List all parties, including IT, that will have access to the data. Make sure this list is always up to date.
- ❑ If outside collaborators will be granted access, explain how this will be done. List the information they will have access to and any agreements you have in place.
- ❑ Specify whether participants will be given a research code number to protect their identity when using this technology.

Storage of research data:

- ❑ Specify where the data will be stored and who will have access to it. Data should be kept in a secure location, a place only the PI and authorized research staff can access (both electronically and physically).
- ❑ Indicate how the data will be protected.
- ❑ Remove necessary subject identifiers from data files, and encrypt data files if stored electronically. Identifiers should be stored in a physically separate and secure location from the

data files, and associated with the data files through a key code that is also stored in a separate and secure location. Additional justification must be provided to rationalize retention of subject identifiers to meet the specific needs of the research study.

- ❑ Specify whether the data will be stored or transmitted immediately. If not transmitted immediately, explain.

Sharing and transferring research data:

- ❑ Fully describe any third-party involvement, including access to and/or retention of the data, and their plans for use or reuse. Make sure to in the informed consent document.
- ❑ Specify which data is transmitted to a server, and indicate if that exchange is encrypted. See the *Guidance on When to Encrypt Data*.
- ❑ Indicate which secure modes of transmission of data will be used (e.g., VPN, secure file transfer, etc.).
- ❑ Data submitted electronically and/or subject identifiers submitted over a public network must be encrypted.

Research data destruction and minimizing potential risks to subject's confidentiality:

- ❑ Explain where the data will go when the study is over (e.g., deleted from the shared folders, de-identified and stored for future use, etc.).
- ❑ If the data will be destroyed, explain how this will be done and by whom and provide an estimated timeline.
- ❑ Specify at what point subject identifiable data will be de-identified or destroyed.

B. Consult with IT to review the technology, institutional policies, and any required agreements:

Begin communicating with IT early in the process, as they will need to conduct their own review of the technology. This can sometimes include working with the technology provider on use agreements.

Review the technology and account:

- ❑ Review your institution's policy on security controls and safeguarding data. Determine whether data can be loaded onto storage devices such as servers, disks, or portable media. Ensure secure transmission of data within an institution, and review how data saved on the institutional server should be properly deleted.
- ❑ Conduct a risk assessment on the technology. Review the chosen survey technology and determine if another survey tool would better fit the research study objectives.
- ❑ Determine the electronic and physical storage methods. Specify how data will be stored or transmitted.
- ❑ Review needs for encryption. Ensure appropriate encryption is in place (e.g., mail, internet, etc.). Determine plan(s) to prevent interception of data by a third party. See the *Guidance on When to Encrypt Data*.
- ❑ Determine if the technology has the capability to verify access, how access will be monitored, what data and subsets of data require research access.

Review the servicer and account:

- ❑ Review and verify the security standards of the survey tool servicer. .
- ❑ Determine who owns the data and how much data will be stored. Determine if the servicer charges by the amount of data. Determine if there are additional costs to protect data.

Determine whether the servicer will destroy the data or re-write the data and at what point the data will be destroyed.

- ❑ Determine whether the servicer will return the data, if yes, how this is done.
- ❑ Determine whether the server is stored outside the US and whether the information is subject to international or export restrictions.

Consult with appropriate individuals and/or offices, which may include IT and legal, to determine if the technology will require a Business Associate Agreement (BAA): The majority of services require that you sign their terms and conditions prior to using the service. When possible, try to negotiate a contract with the servicer.

- ❑ Review the policy to understand how your research might be affected if another company buys the service provider. Determine if the sale would affect the data ownership, disaster recovery, privacy policies, or other issues.
- ❑ The terms of services should address the following:
    - ❑ Privacy rules and regulations
    - ❑ Safety of non-public information (SSN, credit card information, etc.)
    - ❑ Value of intellectual property
    - ❑ Any grant funding requirements regarding security, human subjects privacy regulations, or confidentiality.
- ❑ If applicable, address who reviews the BAA, and who will continue to review updates of the agreement.

3e. Cloud Service and Storage

What is a cloud service and storage technology?

Cloud service and storage generally refers to a set of technologies that enable the collection, and processing and storage of data through a set of services or infrastructure where a third-party vendor manages computing resources on behalf of a data customer. Cloud computing services are ever evolving. While there are many types of configurations, the **cloud** may best be understood as a diverse network of computing resources (e.g., servers, smart phones, PCs, tablets) linked through the internet, which may be used in concert to perform a given set of computing tasks. Through the internet, cloud services can leverage massive data centers and a variety of software capabilities around the world, enabling flexible, scalable, and interoperable access to data and data services from any location. Commonly used cloud service and storage companies include Google Cloud, Amazon Web Services (AWS), Microsoft Azure, Dropbox, Netflix, Flickr, Syncplicity for EMC, and Microsoft 365.

Prior to submitting an IRB application or amendment for research studies using cloud service and storage technology, the following risks and technology considerations should be addressed:

Information risks associated with cloud services and storage can arise because the technology functions over a wireless network and through a third-party platform, making the communication susceptible to wiretapping or interception of data. The sensitivity of the data being collected must be considered when determining the risks to subjects' privacy and confidentiality. Be conservative about storing critical information in the cloud; without an appropriate contract, you should only use cloud storage for information that can be replaced with little or no consequence. In determining the best servicer, consider effective management controls (e.g., oversight of third parties, adequate insurance, disaster recovery, etc.). Also, consider the possibility that another company might purchase the cloud servicers and how that would affect data stored in the cloud service provider (e.g., data ownership, disaster recovery, privacy policies, etc.). Assess the relevance of federal privacy regulations, federal laws, contractual obligations, and grant restrictions before moving institution-related files and data to any cloud server. For financial reasons, many cloud providers locate some of their servers outside the US. In this case, since you won't know the physical location of the servers on which a provider stores your information, you should exercise caution if any of the information you store in the cloud is subject to any international or export restrictions.

Important risks associated with cloud service and storage technology:

1. **Data Ownership** – Research data collected and stored on cloud service and storage technologies is typically owned and/or governed by the investigator's institution or by the sponsor of the research. Factors affecting 'ownership' status includes, among others, who contributed the data, agreements associated with data creation and distribution, contract terms, and intellectual property rights. A cloud service provider may include terms in its vendor contract or end user license agreement (EULA) that automatically transfers some or all ownership rights to the provider. Failure to properly review the contracts and agreements may result in unintentional forfeiture of intellectual property rights or inability to retrieve data. Understand the cloud vendor access and data rights. The two categories of cloud data are data created by the user before uploading it in the cloud and data created on the cloud platform itself.
2. **Data Collection**- Cloud service and storage technology collects data manually with wired or

wireless access to the server. During collection, there may be risks to the confidentiality, integrity, and availability of data.

3. **Data Access**- Data may be accessed in different locations. If data is accessed on a personal device, additional risks may be considered (e.g., the terms of agreement for the personal device were accepted under personal terms not considering the use for research). Additional precautions should be in place to protect the information (e.g., password protected login, ability to logoff users after a set time, ability to lock access if password is entered incorrectly over a set amount of times, etc.). In some cases, users may opt in or opt out of services but by doing this, may sacrifice access to services and data. If opting into cloud service and storage, choose only the minimum services necessary, and limit the number of staff who can access the media. Cloud storage media may allow for password protected access and remote locking capabilities.
4. **Data Storage**- Data should be stored on the appropriate cloud storage technology specified to protect the sensitivity of the data, with appropriate access requirements. Data storage should not be done in personal accounts; you should set up new accounts specifically for the research study. Access rights should be defined for all folders and files in the cloud storage media (e.g., only select research staff have the authority to modify backup files). Remove necessary subject identifiers from data files, and encrypt data files. Identifiers should be stored in a physically separate and secure location from the data files, and associated with the data files through a key code that is also stored in a separate and secure location. There is also the risk of more information being stored than is necessary. Server ports should be actively monitored and secured as they pose a disclosure risk through the exposure on internet search engines (e.g., Google, Yahoo, etc.). The longer data are left unused in storage, the more likely unauthorized individuals outside the network can retrieve it. Regulations have requirements on how data can be accessed and where it can be stored. For example, it is not appropriate to store data regulated by the Health Insurance Portability and Accountability Act (HIPAA) or the Family Educational Rights and Privacy Act (FERPA) in DropBox or other cloud services.
5. **Data Transmission**- Data is transmitted when the cloud service and storage media account is accessed and a data transfer request is made (e.g., request to download, share files, etc.). Risks include access by unauthorized users, mishandling of data, and failure to log out from the media when no longer in use. Whenever possible, don't transfer files via email; instead use an encrypted USB or external drive. When using email, never use your personal email account, as it is not secure. Make sure your work email is set up to be secure. To ensure the security of data being transmission, you can type in the subject line "[send secure]" in front of the subject title. Never include PHI in the subject title; subject titles are not secure. Check the technology to see if the channels are encrypted, secured, and how often the software is updated and patched. Whenever possible, don't transfer files via email; instead use an encrypted USB or external drive. When using email, never use your personal email account as it is not secure. Make sure your work email is set up to be secure. To ensure data being transmitted is secure, you can type in the subject line "[send secure]" in front of the subject title to make the email secure. Never include PHI in the subject title, the subject title is not secure.
6. **Data Sharing**- Data sharing on cloud service and storage technology should be limited by proper access controls (e.g., password protection, encrypted files, etc.). Prior to sharing data, ensure the location and method for sharing is secured and protected based on the sensitivity of the data. A cloud provider may be configured to include protections, but if the researcher downloads or syncs that data to their end device such as a laptop or smartphone, the device may not be secure.
7. **Data Retention and Destruction-** The duration of time the data will be stored on the cloud service and storage media should be taken into account when determining the risks. The media

should be reviewed to determine if reading is possible while the data is being stored. This is especially critical for long-term storage or archiving. Account for the fact that cloud storage media products can have varied shelf lives, and may become obsolete. Depending on the cloud storage company policy, they may have rights to the data, including how the data will be retained and destroyed.

To **eliminate, mitigate, and/or reduce risk,** investigators can communicate with IT, research computing, or information security to ensure that for the research study, network infrastructures have appropriate physical safeguards, access controls (collect and access only the minimum necessary information to conduct the study), and encryption in place.

To mitigate the risk of mishandling private information, investigators and IRBs must consider the risks associated with cloud service and storage, and evaluate and implement methods to reduce these risks.

A researcher can take steps to ensure data protection and privacy by sharing with institutional IT and research compliance all of the written and oral agreements and understandings they have with respect to pre-existing research data and data intended for collection. Researchers should work collaboratively with IT and research computing groups to design infrastructure that protects the data and advances the research. Research data with restrictions on the participation of foreign nationals, publication (prior approval or prior review), or imposed by non-disclosure agreements should not be stored on a commercial cloud service.

The cloud service and storage technology should afford adequate privacy and confidentiality protections, and ensures that additional risks related to cloud service and storage are minimized. The IRB should determine whether they want researchers to explicitly note in the consent form the storage location, or simply specify how the data will be protected. Noting the verbage, “cloud storage” can cause confusion to some subjects.

Appendix: Considerations to eliminate, mitigate, or reduce risk related to the use of *cloud service and storage* technologies in research:

A. When developing research study design and methods, describe procedures and safeguards for:

Collecting and recording research data:

- ❑ Explain your selection criteria for the cloud service and storage vendor in the research protocol. See the *Points to Consider When Choosing a Cloud Service Provider*.
- ❑ Provide detailed information about what the cloud service and storage technology does and its role in the study. Include information about the technology manufacturer, if applicable, such as a brochure, screen shots, version dates, or other information for reviewers.
- ❑ Specify if research data will be created before uploading to the cloud or if the data be created on the cloud platform itself.
- ❑ Indicate whether the cloud service and storage access is by invitation only, with a code (login/password), or if it is available to the public.
- ❑ Explain whether the cloud service and storage will be password-protected.
- ❑ Describe the method of data collection (e.g., survey, uploading of pre-existing database) and how often the data will be collected. Specify whether the data will be transmitted to a server behind your institution's firewall or to another site.
- ❑ Provide the account information the data will be collected and stored under. Do not store research data in personal accounts; use only a business account.
- ❑ Explain how the participant will be informed that the data is subject to the cloud service or storage technology's terms of agreement, and told how these terms may change over time.

Processing, coding, and maintaining access to research data:

- ❑ Specify where and under which conditions individuals will have access to the data (what will be made available and to whom).
- ❑ List all parties, including IT, that will have access to the data. Make sure this list is always up to date.
- ❑ If outside collaborators will be granted access, explain how this will be done. List the information they will have access to and any agreements you have in place.
- ❑ List all vendor certifications.
- ❑ Specify whether participants will be given a research code number to protect their identity when using this technology.

Storage of research data:

- ❑ Specify where the data will be stored and who will have access to it. Data should be kept in a secure location, a place where only the PI and authorized research staff has access (both electronically and physically).
- ❑ Indicate how the data will be protected.
- ❑ Remove necessary subject identifiers and encrypt data files. Identifiers should be stored in a physically separate and secure location from the data files, and associated with the data files through a key code that is also stored in a separate and secure location. Additional justification must be provided to rationalize retention of subject identifiers to meet the specific needs of the research team.

- ❑ Explain plans for cloud service and storage rental costs.

Sharing and transferring research data:

- ❑ Fully describe the cloud service and storage provider involvement, including access, data retention and plans for use or reuse. Make sure to include in the informed consent document.
- ❑ Specify which data is transmitted to a server and if that exchange is encrypted. See the *Guidance on When to Encrypt Data*.
- ❑ Indicate which secure modes of transmission will be used (e.g., VPN, secure file transfer, etc.).

Research data destruction and minimizing potential risks to subject's confidentiality:

- ❑ Explain where the data will go when the study is over (e.g., deleted from the shared folders, de-identified, and stored for future use).
- ❑ If the data will be destroyed, explain how this will be done and whom, and provide an estimated timeline.
- ❑ Specify at what point subject identifiable data will be de-identified or destroyed.

B. Consult with IT to review the technology, institutional policies, and any required agreements

Begin communicating with IT early in the process, as they will need to conduct their own review of the technology. This can sometimes include working with the technology provider on use agreements.

Review the technology and account:

- ❑ Review your institution's policy on security controls and safeguarding data. Ensure secure transmission of data within an institution, and review how data saved on the institutional server should be properly deleted.
- ❑ Conduct a risk assessment on the technology. Review the chosen cloud service and storage technology and determine if another technology would better fit the research study objectives.
- ❑ Determine the electronic and physical storage methods. Specify how data will be stored or transmitted.
- ❑ Review needs for encryption. Ensure appropriate encryption is in place (e.g., mail, internet, etc.).Determine plan(s) to prevent interception of data by a third party. See the *Guidance on When to Encrypt Data*.
- ❑ Specify how access will be monitored and identify which data and subsets of data require research access.

Review the servicer and account:

- ❑ Review and verify the security standards of the cloud service and storage technology provider.
- ❑ Determine who owns the data and how much data will be stored. Determine if the technology provider charges by the amount of data. Determine if there are additional costs to protect the data.
- ❑ Determine whether the technology provider will destroy the data or re-write the data and at what point the data will be destroyed.
- ❑ Determine whether the technology provider will return the data, and if yes, how this is done.
- ❑ Determine whether the server stored is outside the US, and whether the information is subject to international or export restrictions.

Consult with appropriate individuals and/or offices, which may include IT and legal, to determine if the technology will require a Business Associate Agreement (BAA): The majority of services require that you sign their terms and conditions prior to using the service. When possible, try to negotiate a contract with the servicer.

- ❑ Review the policy to understand how your research might be affected if another company buys the service provider. Determine if the sale would affect the data ownership, disaster recovery, privacy policies, or other issues.
- ❑ The terms of service should address:
  - ❑ Privacy rules and regulations
  - ❑ Safety of non-public information (SSN, credit card information, etc.)
  - ❑ Value of intellectual property
  - ❑ Any grant funding requirements regarding security, human subjects privacy regulations or confidentiality.
- ❑ If applicable, identify who reviewed the BAA, and who will continue to review updates of the agreement.

Contract with Cloud Service Provider:

- ❑ Include the right to audit and inspect the technology provider's data security practices (e.g., third-party audit reports).
- ❑ Where human subject protections and data privacy law apply, ensure that the technology provider is contractually bound to apply data protection safeguards that meet the researchers' obligations under contract or law (e.g., HIPAA requirement to execute business associate agreements with subcontractors).
- ❑ Ensure that the technology provider adheres to most current data security frameworks that apply administrative, physical, and technical safeguards (e.g., FISMA, ISO 27001, NIST 800-53).
- ❑ Confirm that technology provider can comply with contractual or legal obligations on data access (e.g., reports on disclosures or law enforcement access).
- ❑ Determine the roles and responsibilities of the researcher, research institution, and cloud service provider.
- ❑ Review the cloud service provider's capacity to comply with conditions of IRB oversight and human subject protection regulations.

4. Additional Resources

4a. Investigator Checklist for Securing Research Data

- Ensure that the website where you are typing your login credentials (username and password) uses **SSL** (secure socket layers). You can determine this by looking at the web page address. It should begin with **https://** or display an icon of a padlock beside the URL.
- Remember to create strong passwords. Avoid using words found in any dictionary.[16] Combine mixed case and symbol(s), and make the password at least six characters. Use a unique password for each account. Consider two factor authentication/multi-factor authentication on sensitive accounts, where available. Password managers (such as LastPass or 1Password) may be used to securely store your passwords. Additional passwords guidelines may be given by your IT department.
- Whenever possible, avoid storing subject identifiable data on portable devices such as laptop computers, digital cameras, portable hard drives including flash drives, USB memory sticks, iPods, smartphones or similar storage devices, as they are particularly susceptible to loss or theft. If it is necessary to use portable devices for initial collection of subject identifiers, the data files must be encrypted, and subject identifiers transferred to a secure system as soon as possible and securely deleted from the device after transfer.
- Ensure your workstations are limited to authorized users who have appropriate validation
    - Designate a secure location with limited access for paper-based records
    - Prior to receipt of study-related information, set up access privileges and passwords.
- Questions to ask when sharing access to online folders:
    - Does the person have read-only access or are they authorized to change or delete the folder?
    - Will you have the ability to know when the files are accessed and changes are made?
    - Who will you be sharing the file with? Have they been listed/approved to access the data? Who is responsible for managing the administrative access of the folders? Are the folders password-protected? Are they on a secure network?[17]
- Restrict access to the following areas to increase the security of private data:

1. Ensure your physical environment is secure:
    - ❑ Lock offices or work area(s).
    - ❑ Secure laptops at desks/workstations (use a cable lock when possible).
    - ❑ Keep paper files containing private data in locked file cabinets and/or in locked offices.
    - ❑ Retrieve immediately print-outs and faxes that contain private data.
    - ❑ Make sure computers are not left unattended for long periods of time, and turn off when no longer in use.
    - ❑ Always dispose of documents containing private information by shredding or placing in secure, confidential recycling bins (check with your institution regarding any questions about disposal).

[16] http://www.american.edu/oit/security/IRB-Mobile-Phone.cfm

[17] http://www.albany.edu/orrc/assets/Institutional_Review_Board_Data_Management_Policy_v_1_0.pdf

- ❑ Adjust your monitor or use a screen filter to protect private data from prying eyes.

2. Secure your technical environment:
    - ❑ Use strong passwords and never share them with others.
    - ❑ Changes to computer settings can cause changes in security; consult with IT before changing settings.
    - ❑ Secure workstations by:
        - Installing anti-virus software and set it to update automatically.
        - Install a password-protected screen saver.
        - Turn on automatic updates to keep computer operating systems (e.g. MS Windows, MAC OSX) current.
        - Enable automatic updates for other software such as Adobe and Acrobat.
        - Enable a firewall for your operating system.
3. Learn your work processes:
    - ❑ Learn and apply your institution policy and procedural requirements for safeguarding data.
    - ❑ Update your knowledge of safe computing practices.
    - ❑ Understand the risks associated with an inadequately secured work area.
    - ❑ Be discreet when leaving audio messages about private matters.
    - ❑ Always report security violations to IT, your supervisor, or the appropriate office at your institution.

4. Take steps to securing your email, internet, and home computer:
    - ❑ Never open an email attachment from an unknown source. If you know the sender but the email still seems suspicious, you may want to contact the sender to verify the attachment before opening.
    - ❑ Do not use personal email accounts to send work-related information.
    - ❑ Report any email with urgent requests for personal financial information to IT.
    - ❑ Contact IT if you use your home computer to access systems containing personal information as it's important to keep your computer secure and regularly update your software.

4b. Guidance on When to Encrypt Data [18]

What is encryption?

Encryption is the conversion of data into a format that is not easily understood by unauthorized viewers. Encryption can be applied to storage devices (data "at rest") and to network data (data "in transit"). The type of computing device and network communicating from/to, and if personal or Protected Health Information (PHI) is involved will dictate whether or not encryption is required.

Encryption is not necessary if you do not store or work with research data that includes personal or PHI. Therefore, it is best *not* to collect any of this information unless it is actually necessary. Always contact your help desk to ensure you are doing everything required. Password-protected is not the same as encryption – you must do both to protect data.

Scenarios in which *storage* encryption is required – possession of research data that includes personal and/or Protected Health Information ***and*** one or more of the following:

- Computing device is a mobile device ***or***
- Computing device is a personal system ***or***
- Storage device is removable (portable) ***or***
- Access to the storage device is not in a physically secure environment.

Scenarios in which *network* encryption is required – usage of research data that includes personal and/or Protected Health Information over a network. The information is not already encrypted by means of storage encryption ***and*** one or more of the following:

- Any part of the data transmission is outside of a trusted network **OR**
- Access to a system containing research data that is personal and/or includes Protected Health Information that is not entirely over a trusted network.

Additional examples when encryption is required – use of electronic research data that includes personal and/or PHI **AND** the information is being sent by:

- Email **OR**
- Webmail **OR**
- Web browser **OR**
- US mail **OR**
- Courier **OR**
- Instant messenger **OR**
- Peer-to-peer network **OR**
- Wireless (wi-fi, smartphone, etc.) **OR**
- Backup of the information is created

[18] Adapted from the University of California, Irvine Office of Research <http://www.research.uci.edu/compliance/human-research-protections/researchers/data-security.html>

4c. Points to Consider When Choosing a Cloud Service[19]

Be diligent when considering using the cloud since it is very complex, covering many different tools, offerings, and configurations. Cloud users need to be informed the line between the provider's responsibilities and their own. In using the cloud, you should be aware of the lifecycle of the researcher's data, tracing where the path of its flow. A cloud provider may offer protections, and be configured to do so, but if the researcher downloads and/or syncs that data to their end device such as a laptop or smartphone the same level of protection is not available. Make sure to become educated the common terms used by cloud providers regarding their options for services. Be aware the terms S**oftware as a Service** (SaaS), **Infrastructure as a Service** (IaaS), and **Platform as a Service** (PaaS). **Defined in the glossary*

1. **Are their security standards appropriate?**
   Make sure that the company has a good reputation and solid security policies. Remember, you are trusting this company to store your personal information. Be sure the level of service matches the sensitivity of the data.

2. **How much data will you be storing?**
   Search with a realistic expectation of the size you need to store all your files. Many companies charge by the amount of storage you are requesting.

3. **Is your data encrypted when being uploaded to, or downloaded from, the cloud?**
   Make sure your browser or app requires an encrypted connection before you upload or download your data. Look for the "https://" or the padlock image beside the URL in your browser.

4. **Is your data encrypted when stored in the cloud?**
   This answer will be in the terms of service, but you can expect your data will be stored on the cloud server with no encryption, which means that anyone who has (or can get) high-level access to that server will be able to read your files. This may not be an issue for some files, but you should carefully consider the information you are storing in the cloud, and whether or not you are comfortable with others accessing it. At a minimum, no data that is protected by law (medical information, personal identifiers, financial data) should be stored in the cloud unless the storage solution is encrypted and you identify who is allowed to decrypt it, and for what reason. Access should only be granted to you or others within your organization.

5. **Understand how access is shared with your cloud folder.**
   Several cloud storage providers allow you to share access to your online folders with other people. Be sure to understand all the details on how this works. Will they be allowed only read -only privileges or can they make edits? Will you know who altered a file last? If you share the file with a group, do you know all the members of the group? Are you notified if the group membership changes? Does the service allow you to make files public? If made

[19] http://www.bu.edu/infosec/howtos/how-to-safely-store-your-data-in-the-cloud/

public, is personal information (name, account, email, etc.) attached to that file for the public to view?

6. **Understand your options if the cloud provider is hacked or loses your data.**
   Cloud services require that you sign their terms and conditions before you can start the service. In the vast majority of cases, these conditions state that you have very little, if any, remedy if there are any data breaches. Be aware of the terms you are agreeing to.

4d. Glossary of Common Terms for Technologies Used in Research

A

Access: The ability to get to what you need. Data access is the ability to get to (usually with permission to use) specific data on a computer. Web access means a connection to the internet through an access provider or an online service provider.

Access marker: Represents a single value or piece of data.

Advanced Encryption Standards (AES): An algorithm designed to encrypt data developed by the US government, these standards are used to protect classified information.

Anti-malware: A software program designed to prevent, detect, and remediate malicious programming on individual computing devices and IT systems.

Application (App): An application is a software program that's designed to perform a specific function directly for the user or, in some cases, for another application program.

B

Box: A service that offers online secure collaboration of file sharing.

Bring your own device (BYOD): A commonly used term that refers to bringing your personally owned device to your workplace and/or to be used to facilitate research.

C

Cache memory: A type of memory to hold frequently used data. Web browsers use cache memory to save copies of previously viewed web pages.

CertainSafe: A service provider that offers secure management of sensitive information.

Cloud computing: As this term relates to research data, it means moving sensitive data out of the healthcare organization and into the data centers of cloud providers, which might be located in multiple regions around the world and subject to a range of local regulations.

Code42: Data protection service that backs up distributed end-user data in a single, secure platform. Also known as the "SaaS" solution.

Common Rule: Basic provisions for IRBs, informed consent and assurances of compliance. Human subject research conducted or supported by each federal department or agency is governed by the regulations of that department or agency.

Confidentiality: Pertains to the treatment of information that an individual has disclosed in a relationship of trust, and with the expectation that it will not be divulged to others without permission and in any ways that is inconsistent with the original disclosure.

Containerization: A lightweight alternative to full-machine virtualization (virtual version of a device or resource) that involves encapsulating an application into a container with its own operating environment.

Cookies: A text file placed on a user's computer by a website or web server. Often used to keep track of individuals as they navigate a site, and more broadly, the web.

CrashPlan: A private and public cloud-based service that is a data backup solution accessible from any location.

D

Data: A collection of facts. Data can exist in many different forms and be translated into different forms to help analyze and categorize it.

Data at rest: All data in computer storage, excluding data that is traversing a network temporarily or reference files that are rarely changed. It also refers to data that is subject to regular, but not constant change.

Data collection: A systematic approach to gathering and measuring information from a variety of sources to get a complete and accurate picture of an area of interest.

Data mining: Also called "knowledge discovery" when referring to a database. Refers to the process of discovering interesting and useful patterns and relationships in large volumes of data.

Data in motion: The process of transferring data among all of the original files.

Data retention: The continued storage of data for compliance, also called records retention.

Data subset: A portion of a total data set, generally corresponding to a specific aspect of the data or structure.

Device: In a general context, a device is a machine designed for a purpose, such as a phone or calculator. In the context of computer technology, a device is a unit of hardware that provides input to the computer and/or receives output, such as keyboards, mouse, display monitors, CD-ROM players, printers, audio speaker, microphones, etc.

DOD Information Assurance Certification and Accreditation Process (DIACAP): A systematic process that ensures only accredited information system tools and technologies are used within the US Department of Defense (DoD)'s IT infrastructure.

Disk storage: Storage on a disk using magnetic read/write technology (used for medium to long-term storage).

DropBox: A private serice provider that offers a cloud service for file sharing and collaboration. Allows accounts to be set up for both business and personal use.

E

Encryption: The conversion of electronic data into another form, called "ciphertext", which cannot be easily understood by anyone except authorized parties.

End User License Agreement (EULA): A legal contract between a software application author or publisher, and the user of that application.

External collaborators: Provide a service or resource but are not directly controlled by the person/company that hired them. Examples include: services, repositories, presenters, framework classes, email senders, loggers, and file system wrappers.

Federal Information Processing Standards (FIPS): A set of standards that describe document processing, encryption algorithms, and other information technology standards for use within non-military government agencies and by government contractors and vendors who work with these agencies.

Federal Information Security Management Act (FISMA): US legislation that defines a comprehensive framework to protect government information, operations, and assets against natural or manmade threats.

Federal Risk and Authorization Program (FedRAMP): Federal regulation for cloud providers which allows the government to use a particular cloud system without having to validate physical access

Flash memory: A popular, non-volatile and rewritable memory chip. Extremely durable, flash memory is used in just about every electronic device, including USB drives, cameras, iPods, smartphones, and tablets. In addition, flash-based solid-state drives (SSDs) are increasingly replacing hard disks in laptops, desktops, and servers.

H

Hightail: Formerly YouSendIt, a private cloud service that allows users to send, receive, and digitally sign and synchronize files.

HIPPA: Health Insurance Portability and Accountability Act of 1996 is US legislation that provides privacy standards to protect patients' medical records and other health information provided to health plans, doctors, hospitals, and other healthcare providers.

I

Identifiers: Identifiers are symbols used to uniquely identify a program element in the code. They are also used to refer to types, constants, macros, and parameters.

IDrive: A private cloud-based backup service provider for consumers and small businesses.

Infrastructure as a Service (IaaS): A service model that delivers computer infrastructure on an outsourced basis to support enterprise operations. It provides hardware, storage, servers and data center space or network components, as well as software.

ISO 27001: A specification for an information security management system (ISMS).

L

Local area network (LAN): LAN is a computer network for sharing data and devices within a small geographical area such as a home, school, computer laboratory, or office building(s).

M

Malware attacks: Malicous software that takes over a computer to spread the bug or virus to other

devices.

Man in the middle attack (MitM): In computer security, this term refers to an attacker that secretly intercepts and relays messages between two parties who believe they are communicating directly with each other.

Microsoft One Drive: Formerly SkyDrive, a cloud-based backup service under Windows Essentials, it enables Microsoft account holders to store files, images, and other data online and offline, and sync and access that data from both computers and mobile devices.

Mobile Device Management (MDM): The administrative area dealing with deploying, securing, monitoring, integrating, and managing mobile devices in the workplace.

Mobile Medical Application (MMA): The FDA defines MMA as a "software application that can be executed (run) on a mobile platform or a web-based software application that is tailored to a mobile platform but is executed on a server," where that software already meets the general definition of a medical device as found in 210(h) of the Federal Food, Drug, and Cosmetic (FD&C) Act.

N

National Institute of Standards and Technology (NIST): A non-regulatory federal agency within the US Department of Commerce that promotes innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security.

O

Optical storage: The storage of data on an optically readable medium, meaning it can be read with the aid of light (e.g., CD-ROM).

P

Payment Card Industry Data Security Standard (PCI-DSS): A set of policies and procedures intended to optimize the security of credit and debit transactions, and protect cardholders against misuse of personal information.

Personally Identifiable Information (PII): Any data or information that can be used to distinguish one person from another and could potentially identify a specific individual.

Physical security: The protection of personnel, hardware, programs, networks, and data from physical circumstances and events that could cause serious losses or damage to an enterprise, agency, or institution. This includes protection from fire, natural disasters, burglary, theft, vandalism, and terrorism.

Physical storage: The storage on physical disks within discovered enclosures.

Platform as a Service (PaaS): Cloud computing model that delivers applications over the internet.

Privacy: In regards to data, it is the right to keep personal information protected from the public.

S

Secure File Transfer Protocol (SFTP): A network that enables file access, transfer, and management over a secured file transferring system.

Service Organization Control 2 (SOC2): Audit standards which reports on issues related to security,

availability, processing integrity, confidentiality, or privacy.

Snooping: In a security context, unauthorized access to another person's or company's data.

Software as a service (SaaS): A software distribution model that hosts applications and makes them available to customers over the internet.

Structured Query Language (SQL) injection: A security exploit in which the attacker adds the SQL code to a web form input box to gain access to resources or make changes to data.

Secure Socket Layer (SSL): A technology that manages server and client authentication to establish encrypted transmission of communications over the internet.

SSL Encryption: A popular implementation of public-key encryption.

Storage device: Any computing hardware used for storing, porting, and extracting data files and objects.

Store data or data store: A repository for data such as a database, file system, or directory.

SugarSync: A private online sync-and-share files service for users to upload, access, and share files.

T

Tape storage: Storage using magnetic reel tape often used for archives or backup.

Third party: Web-based technologies that provide services for payment. Often a third-party service agreement is negotiated and signed, defining the terms and conditions for the services. For more information on third-party services please see the Federal Trade Commission website.

Transmit data or data transmission: The process of sending digital data to computing, network, communication, or electronic devices.

U

Uniform resource locator (URL): The global address of documents and other resources on the world wide web.

V

Virtual machine: In regards to computers, a virtual machine is an emulation of a particular computer system.

Virtual private network (VPN): A private network built over a public infrastructure that allows users to securely access the network on the internet.

Volatility of storage: Extent to which data may be lost if power is lost.

W

Web beacon: An embedded object in a web page or email that is typically transparent and tracks behavior or use of the web page or email. Web beacons can be detected by looking for tags that load from an alternate server then. Often web beacons are embedded with cookies.

Wi-Fi Protected Access (WPA): An improved security standard for computers equipped with wi-fi.

5. Attribution, Sharing, and Adapting

We encourage you to:

- **Request** – email us and request the materials
- **Share** – copy, distribute, and transmit the work
- **Adapt** – adapt the work to suit your needs
- **Contribute** – share your guidance or best practices on technologies listed in the document or new technologies to add.

Under the following conditions:

- **Attribution:** We encourage the broad dissemination of this tool. In freely using the materials or when citing this tool, we require that you acknowledge Harvard Catalyst | The Harvard Clinical and Translational Science Center as the publisher, and that you give appropriate credit to any individual authors.

- **Suggested citation:** *This material is the work of the Harvard Catalyst IRB-IT Task Force of the Regulatory Foundations, Ethics, and Law Program. This work was conducted with support from Harvard Catalyst | The Harvard Clinical and Translational Science Center (National Center for Research Resources and the National Center for Advancing Translational Sciences, National Institutes of Health Award 8UL1TR000170-05 and financial contributions from Harvard University and its affiliated academic healthcare centers). The content is solely the responsibility of the authors, and does not necessarily represent the official views of Harvard Catalyst, Harvard University, and its affiliated academic healthcare centers, or the National Institutes of Health.*

With the understanding that:

- **We might contact you:** We are interested in gathering information on those who are using these materials and how they are using it. We may contact you by email about this, or to request collaborations or input on future activities.
- **When reusing or distributing, make clear the above terms:** For any reuse or distribution, you must make clear to others the terms of this work. The best way to do this is include the web link for this guide.
- **When adapting:** Please share improvements you've made to this guide with us so that we may learn from your feedback, and modify our materials.

6. Acknowledgments and Contact Us

7. Bibliography

"About Us - Free the World's Creativity." Hightail. Hightail, n.d. Web. 24 May 2016. <https://www.hightail.com/about>.

"CertainSafe® Digital Vault - Advanced Cyber Security For Data At Rest And In Motion." Certain Safe. Web. 08 Apr. 2016. <https://certainsafe.com/>.

"Definitions for Physical Storage Terms." Veritas, 21 Oct. 2015. Web. 20 May 2016. <https://www.veritas.com/support/en_US/article.000062514>.

"Federal Policy for the Protection of Human Subjects ('Common Rule')." HHS.gov. 18 Mar. 2016. Web. 25 Apr. 2016.

"HIPAA." MedicineNet. 14 June 2012. Web. 06 Apr. 2016. <http://www.medicinenet.com/script/main/art.asp?articlekey=31785>.

"IDrive Inc. Is an Online Backup Service Provider, Based in Calabasas, CA." IDrive. IDrive, n.d. Web. 25 May 2016. <https://www.idrive.com/online-backup-company>

"Indiana University Indiana University Indiana University." What Is SFTP, and How Do I Use It to Transfer Files? 17 Feb. 2016. Web. 06 Apr. 2016. <https://kb.iu.edu/d/akqg>.

"Privacy and Confidentiality." Privacy and Confidentiality. University of California, Irvine Office of Research. Web. 06 Apr. 2016. <http://www.research.uci.edu/compliance/human-research protections/researchers/privacy-and-confidentiality.html>.

"Q & A: What Is Meant by the Terms Data at Rest and Data in Motion?" What Is Meant by the Terms Data at Rest and Data in Motion? Waytek, n.d. Web. 20 May 2016. <http://waytek.com/q-what meant-terms-data-rest-and-data-motion>.

"Third-Party Services." Third-Party Services. Federal Trade Commission, 31 Mar. 2016. Web. 06 Apr. 2016. <http://www.ftc.gov/site-information/privacy-policy/third-party-services>.

"We Are Code42." Code42 - Protecting & Managing Your Digital Life. Code42, n.d. Web. 24 May 2016. <http://www.code42.com/about/>.

"What Is a Local Area Network (LAN)? - Definition from Techopedia." Techopedia.com. Techopedia, n.d. Web. 20 May 2016. <https://www.techopedia.com/definition/5526/local-area-network-lan>.

"What Is a Storage Device? - Definition from Techopedia. Techopedia.com." Techopedia, n.d. Web. 20 May 2016. <https://www.techopedia.com/definition/1119/storage-device>.

"What Is a Virtual Machine (VM)? - Definition from Techopedia." Techopedia.com. Techopedia, n.d. Web. 20 May 2016. <https://www.techopedia.com/definition/4805/virtual-machine-vm>.

"What Is a Virtual Private Network (VPN)? - Definition from Techopedia." Techopedia.com. Techopedia, n.d. Web. 20 May 2016. <https://www.techopedia.com/definition/4806/virtual-private-network-vpn>.

"What Is an Identifier? - Definition from Techopedia." Techopedia.com. Techopedia, n.d. Web. 20 May 2016. <https://www.techopedia.com/definition/1810/identifier-c>.

"What Is Cache?" What Is Cache? Computer Hope. Web. 08 Apr. 2016. <http://www.computerhope.com/jargon/c/cache.htm>.

"What Is Data Transmission? - Definition from Techopedia." Techopedia.com. TechTarget, n.d. Web. 20 May 2016. <https://www.techopedia.com/definition/9756/data-transmission>.

"What Is DOD Information Assurance Certification and Accreditation Process (DIACAP)? - Definition from Techopedia." Techopedia.com. N.p., n.d. Web. 20 May 2016. <https://www.techopedia.com/definition/25825/dod-information-assurance-certification-and accreditation-process-diacap>.

"What Is Infrastructure as a Service (IaaS)? - Definition from Techopedia." Techopedia.com. Techopedia, n.d. Web. 20 May 2016. <https://www.techopedia.com/definition/141/infrastructure-as-a service-iaas>.

"What Is SkyDrive? - Definition from Techopedia. Techopedia.com." Techopedia, n.d. Web. 20 May 2016. <https://www.techopedia.com/definition/29075/skydrive>.

"What Is Volatile Storage? - Definition from Techopedia." Techopedia.com. Techopedia, n.d. Web. 20 May 2016. <https://www.techopedia.com/definition/9966/volatile-storage>.

Barnett, Emma. "What Is the Difference between Spam, Malware and Phishing?" The Telegraph. Telegraph Media Group, 19 Jan. 2011. Web. 20 May 2016. <http://www.telegraph.co.uk/technology/8267578/What-is-the-difference-between-spam malware-and-phishing.html>.

Beal, Vangie. "Data." What Is Data? Webopedia Definition. Webopedia. Web. 08 Apr. 2016. <http://www.webopedia.com/TERM/D/data.html>.

Beal, Vangie. "NIST." What Is ? Webopedia Definition. Webopedia, n.d. Web. 20 May 2016. <http://www.webopedia.com/TERM/N/NIST.html>.

Beal, Vangie. "URL - Uniform Resource Locator." What Is URL (Uniform Resource Locator)? Webopedia Definition. N.p., n.d. Web. 20 May 2016. <http://www.webopedia.com/TERM/U/URL.html>.

Beal, Vangie. "Web Beacon." What Is Web Beacon? Webopedia Definition. Webopedia. Web. 06 Apr. 2016. <http://www.webopedia.com/TERM/W/Web_beacon.html>.

Beal, Vangie. "What Is Cloud Computing? Webopedia Definition." What Is Cloud Computing? Webopedia Definition. Web. 06 Apr. 2016. <http://www.webopedia.com/TERM/C/cloud_computing.html>.

Brandt, Jeffrey L., and Stacie Durkin. "Mobile Medical App & Medical Device Regulations." Mobile Medical App & Medical Device Regulations. Healthcare Information and Management Systems. Web. 06 Apr. 2016. <http://www.himss.org/ResourceLibrary/GenResourceDetail.aspx?ItemNumber=30334>.

Clifton, Christopher. "Data Mining." Encyclopedia Britannica Online. Encyclopedia Britannica, n.d. Web. 20 May 2016. <http://www.britannica.com/technology/data-mining>.

Delvaux, Damien. "Data Subset Management." Damien DELVAUX De FENFFE, Apr. 2010. Web. 20 May 2016. <http://www.damiendelvaux.be/Tensor/UserGuides/Win_Tensor-UserGuide_Subset_Management.pdf>.

Disk Storage. Definition of “disk Storage”. Collins English Dictionary, n.d. Web. 20 May 2016. <http://www.collinsdictionary.com/dictionary/english/disk-storage>.

Internet-Based Research-CPHS University of California, Berkley Cphs.berkeley.edu/internet_research.pdf. Berkeley, CA: University of California, Berkeley, 07 July 2015. PDF.

IT@Cornell. "IT: Working Definition of Privacy." TeachPrivacy, LLC, 17 May 2011. Web. 20 May 2016. <http://www.it.cornell.edu/policies/infoprivacy/definition.cfm>.

Ross, Tim. "Internal And External Collaborators." Tim Ross Software Developer. WorldPress, 02 Sept. 2009. Web. 20 May 2016. <https://timross.wordpress.com/2009/09/02/internal-and-externa-l collaborators/>.

Rouse, Maragret, and Ivy Wigmore. "What Is BYOD (bring Your Own Device)? - Definition from WhatIs.com." WhatIs.com. TechTarget, Oct. 2012. Web. 08 Apr. 2016. <http://whatis.techtarget.com/definition/BYOD-bring-your-own-device>.

Rouse, Maragret, and Michael Cobb. "What Is Advanced Encryption Standard (AES)? - Definition from WhatIs.com." SearchSecurity. TechTarget, Nov. 2014. Web. 08 Apr. 2016. <http://searchsecurity.techtarget.com/definition/Advanced-Encryption-Standard>.

Rouse, Maragret. "What Is Access? - Definition from WhatIs.com."WhatIs.com. TechTarget, Aug. 2005. Web. 08 Apr. 2016. <http://whatis.techtarget.com/definition/access>.

Rouse, Maragret. "What Is Data at Rest? - Definition from WhatIs.com." SearchStorage. TechTarget, Aug. 2010. Web. 08 Apr. 2016. <http://searchstorage.techtarget.com/definition/data-at-rest>.

Rouse, Maragret. "What Is Secure Sockets Layer (SSL)? - Definition from WhatIs.com." SearchSecurity. TechTarget, Nov. 2014. Web. 06 Apr. 2016. <http://searchsecurity.techtarget.com/definition/Secure-Sockets-Layer-SSL>.

Rouse, Margaret. "What Is Antimalware (anti-malware)? - Definition from WhatIs.com." SearchSecurity. TechTarget, Nov. 2013. Web. 20 May 2016. <http://searchsecurity.techtarget.com/definition/antimalware>.

Rouse, Margaret. "What Is App? - Definition from WhatIs.com." SearchMobileComputing. Nov. 2011. Web. 08 Apr. 2016. <http://searchmobilecomputing.techtarget.com/definition/app>.

Rouse, Margaret. "What Is Box (Box.net)? - Definition from WhatIs.com." SearchMobileComputing. TechTarget, June 2012. Web. 20 May 2016. <http://searchmobilecomputing.techtarget.com/definition/Box-Boxnet>

Rouse, Margaret. "What Is Data Collection? - Definition from WhatIs.com." SearchCIO. TechTarget, May 2016. Web. 20 May 2016. <http://searchcio.techtarget.com/definition/data-collection>.

Rouse, Margaret. "What Is Data Retention? - Definition from WhatIs.com." SearchStorage. TechTarget, Feb. 2014. Web. 20 May 2016. <http://searchstorage.techtarget.com/definition/data-retention>.

Rouse, Margaret. "What Is Data Store? - Definition from WhatIs.com." WhatIs.com. TechTarget, June 2013. Web. 20 May 2016. <http://whatis.techtarget.com/definition/data-store>.

Rouse, Margaret. "What Is Device? - Definition from WhatIs.com." WhatIs.com. TechTarget, Apr. 2005. Web. 20 May 2016. <http://whatis.techtarget.com/definition/device>.

Rouse, Margaret. "What Is Dropbox? - Definition from WhatIs.com." SearchMobileComputing. TechTarget, Nov. 2011. Web. 20 May 2016. <http://searchmobilecomputing.techtarget.com/definition/Dropbox>.

Rouse, Margaret. "What Is Encryption? - Definition from WhatIs.com." SearchSecurity. TechTarget, Nov. 2014. Web. 20 May 2016. <http://searchsecurity.techtarget.com/definition/encryption>

Rouse, Margaret. "What Is End User License Agreement (EULA)? - Definition from WhatIs.com." SearchCIO. TechTarget, Sept. 2005. Web. 20 May 2016. <http://searchcio.techtarget.com/definition/End-User-License-Agreement>.

Rouse, Margaret. "What Is Federal Information Security Management Act (FISMA) ? - Definition from WhatIs.com." SearchSecurity. TechTarget, May 2013. Web. 20 May 2016. <http://searchsecurity.techtarget.com/definition/Federal-Information-Security-Management-Act>.

Rouse, Margaret. "What Is Federal Risk and Authorization Program (FedRAMP)? - Definition from WhatIs.com." WhatIs.com. TechTarget, May 2014. Web. 20 May 2016. <http://whatis.techtarget.com/definition/Federal-Risk-and-Authorization-Program-FedRAMP>.

Rouse, Margaret. "What Is FIPS (Federal Information Processing Standards)? - Definition from WhatIs.com." WhatIs.com. TechTarget, Mar. 2011. Web. 20 May 2016. <http://whatis.techtarget.com/definition/FIPS-Federal-Information-Processing-Standards>.

Rouse, Margaret. "What Is Flash Memory ? - Definition from WhatIs.com." SearchStorage. TechTarget, Mar. 2015. Web. 20 May 2016. <http://searchstorage.techtarget.com/definition/flash-memory>.

Rouse, Margaret. "What Is ISO 27001? - Definition from WhatIs.com." WhatIs.com. TechTarget, Sept. 2009. Web. 20 May 2016. <http://whatis.techtarget.com/definition/ISO-27001>.

Rouse, Margaret. "What Is Man-in-the-middle Attack (MitM)? - Definition from WhatIs.com." IoT Agenda. TechTarget, Dec. 2015. Web. 20 May 2016. <http://internetofthingsagenda.techtarget.com/definition/man-in-the-middle-attack-MitM>.

Rouse, Margaret. "What Is Mobile Device Management (MDM)? - Definition from WhatIs.com." SearchMobileComputing. TechTarget, June 2013. Web. 20 May 2016. <http://searchmobilecomputing.techtarget.com/definition/mobile-device-management>.

Rouse, Margaret. "What Is Optical Storage? - Definition from WhatIs.com." SearchStorage. TechTarget, Sept. 2005. Web. 20 May 2016. <http://searchstorage.techtarget.com/definition/optical-storage>.

Rouse, Margaret. "What Is PCI DSS (Payment Card Industry Data Security Standard)? - Definition from WhatIs.com." SearchFinancialSecurity. TechTarget, May 2009. Web. 20 May 2016. <http://searchfinancialsecurity.techtarget.com/definition/PCI-DSS-Payment-Card-Industry-Data-Security-Standard>.

Rouse, Margaret. "What Is Personally Identifiable Information (PII)? - Definition from WhatIs.com." SearchFinancialSecurity. TechTarget, Jan. 2014. Web. 24 May 2016. <http://searchfinancialsecurity.techtarget.com/definition/personally-identifiable-information>.

Rouse, Margaret. "What Is Physical Security? - Definition from WhatIs.com." SearchSecurity. TechTarget, Dec. 2005. Web. 20 May 2016. <http://searchsecurity.techtarget.com/definition/physical-security>.

Rouse, Margaret. "What Is Platform as a Service (PaaS)? - Definition from WhatIs.com." SearchCloudComputing. TechTarget, Jan. 2015. Web. 20 May 2016. <http://searchcloudcomputing.techtarget.com/definition/Platform-as-a-Service-PaaS>.

Rouse, Margaret. "What Is Snooping? - Definition from WhatIs.com." SearchSecurity. TechTarget, June 2007. Web. 20 May 2016. <http://searchsecurity.techtarget.com/definition/snooping>.

Rouse, Margaret. "What Is Soc 2 (Service Organization Control 2)? - Definition from WhatIs.com." SearchCloudSecurity. TechTarget, Apr. 2012. Web. 20 May 2016. <http://searchcloudsecurity.techtarget.com/definition/Soc-2-Service-Organization-Control-2>.

Rouse, Margaret. "What Is Software as a Service (SaaS)? - Definition from WhatIs.com." SearchCloudComputing. TechTarget, May 2016. Web. 20 May 2016. <http://searchcloudcomputing.techtarget.com/definition/Software-as-a-Service>.

Rouse, Margaret. "What Is SQL Injection? - Definition from WhatIs.com." SearchSoftwareQuality. TechTarget, Jan. 2010. Web. 20 May 2016. <http://searchsoftwarequality.techtarget.com/definition/SQL-injection>.

Rouse, Margaret. "What Is SugarSync? - Definition from WhatIs.com." SearchCloudStorage. TechTarget, June 2014. Web. 20 May 2016. <http://searchcloudstorage.techtarget.com/definition/SugarSync>.

Rouse, Margaret. "What Is Wi-Fi Protected Access (WPA)? - Definition from WhatIs.com." SearchMobileComputing. TechTarget, Nov. 2005. Web. 20 May 2016. <http://searchmobilecomputing.techtarget.com/definition/Wi-Fi-Protected-Access>.

Stroud, Forrest. "Containerization?" What Is Containerization? Webopedia Definition. Webopedia. Web. 08 Apr. 2016.