HARVARD
CATALYST

Harvard Clinical & Translational Science Center

Sample Informed Consent Language Library

Describing technologies used in research

Emerging Technologies, Ethics, and Research Data Committee
Harvard Catalyst Regulatory Foundations, Ethics, and Law Program

Table of Contents

This material is the work of the Regulatory Foundations, Ethics, and Law Program, part of the Harvard Catalyst | The Harvard Clinical and Translational Science Center. Funded by NCATS (UL1TR002541).

Overview

Advances in technology and analytical tools enable discoveries that are essential to our understanding of health and disease, and ultimately to the improvement of human health, healthcare delivery, and healthcare technology itself. Because of these advances, the health information and data of research participants are increasingly being collected, stored, and shared using more powerful and prolific technologies. The increased power and ease of these tools, as well as the increased demand for privacy, raise issues of vital concern to prospective research participants.

Research participants contribute their time, data, and health information, and it is fundamental that their rights, welfare, and interests are respected throughout the research process, starting with the process of obtaining informed consent. Investigators must enable prospective subjects to sufficiently understand and make informed decisions concerning the collection and use of their personal data, and the risks and benefits of participation. As part of a research study, a research participant's personal data may:

- Be stored and used indefinitely.
- Be subjected to risks that are uncertain or unclear.
- Be reinterpreted and change in relevance over time.
- Raise privacy concerns, in part because of the risk of re-identification, as well as the possibility of breach of confidentiality.

Investigators must not only consider and address these factors when designing a research study, but also find meaningful and effective ways to describe these and other technology-specific factors within the informed consent process and consent form.

Purpose

This resource provides advanced information and sample language to assist investigators in describing technologies used in research within the informed consent form. Given the complexity of the scientific and ethical issues that arise when conducting human research, this library is not intended to provide universal suggestions or solutions, but rather to provide language that clearly conveys this complex but important information, and which may be adapted on a study-by-study basis.

The sample consent language in this document has been adopted from real-world examples, and provides investigators with a dynamic reference to support the development of appropriate informed consent materials. Investigators should use this resource when developing consent documents in consultation with collaborators and Institutional Review Boards (IRBs), as well as with research participants and communities.

Submit suggestions, ask questions, and share this material by contacting us at regulatory@catalyst.harvard.edu.

This material is the work of the Regulatory Foundations, Ethics, and Law Program, part of the Harvard Catalyst | The Harvard Clinical and Translational Science Center. Funded by NCATS (UL1TR002541).

Chat Technology

Chat technology is a real-time, instant messaging electronic communication between two users, connected by a network. Once a chat has been established, users enter messages that appear on the other user's screen. Many networks and online services offer a chat feature.

Chat technology includes a number of free or paid solutions. Examples of free solutions include SnapChat, Gmail Chat, Skype, and Yahoo! Messenger. Examples of paid solutions include: Velaro, Olark, LiveChat, and SnapEngage. Depending on the technology selected, it can either run as a stand-alone program, web service, or web application.

When communicating with a research participant via online chat that is not part of a videoconference, or by text in general, investigators should consider the inability to observe visual and auditory cues, which could lead to possible problems in interpretation of both questions and responses. Voice intonation and facial expressions are often used to convey and/or emphasize meaning. Thus, investigators may need to ask explicit clarifying questions in order to accurately interpret responses, and provide additional information in order to ensure that potential participants understand questions and information being communicated via a chat session. Another consideration is that a separate language or shorthand has developed around chat technology. If investigators or participants are not familiar with this lingo, chat sessions may generate more confusion than clarity. (See netlingo.com/acronyms.php for a list of acronyms and text shorthand)

Chat technologies used for research purposes are generally not encrypted. The consent should inform research participants that chat sessions are not encrypted or secured during their transmission, and could be intercepted or received from their browser cache.

IRBs often do not have the expertise to evaluate chat technology. Thus, IRBs often require sign off from others to determine whether the chat technologies are suitable for use in research in reference to regulations such as HIPAA and other data privacy laws. If the investigator decides to use a chat service, the service offered by the company should be fully understood and may need to be approved by IT and the IRB for use in research. Keep in mind each chat technology company has its own terms of use agreement and privacy policies. Users must follow rules dictated by the terms of use; some are common sense, while others are based on the company's policies.

Below are model statements investigators may adapt to describe chat technology.

Sample: Chat Messaging - Confidentiality
Your confidentiality will be kept to the degree permitted by the technology being used. Chat messages are not secure when sent in an unencrypted format. First, they can be intercepted (read by others or altered by others), and second, the reader cannot be certain that the sender is who they claim to be.

Sample: Chat Messaging - Encryption
The most effective way of ensuring that what we write will only be read by each other is to use encryption. Some encryption programs are packaged as portable software, which means you can run them from a USB flash drive on any computer. If we communicate without encryption, it is possible that third parties could intercept and read our conversation without our consent. However as long as your

This material is the work of the Regulatory Foundations, Ethics, and Law Program, part of the Harvard Catalyst | The Harvard Clinical and Translational Science Center. Funded by NCATS (UL1TR002541).

information cannot be easily re-identified, any risk to you will be reduced.[1] [If the research team recommends using encryption software, include "ask the research staff about encryption software"].

Sample: Chat Messaging – Use of Different Email Account

For this research study, you may want to set up a new instant messaging account not associated with your full name. Using an instant messaging account that is not linked to your full name (e.g. someguy@hotmail.com) will also provide a degree of confidentiality.

Sample: Chat Message - Storage

Text messages are stored by the telecommunications provider and therefore may not be secure.

[1] "Encryption Guide: Drugs on Forums Project." *Curtin University: NDRI*. Web. 6 Jan. 2016. <http://ndri.curtin.edu.au/drugsonforums/encryption.cfm>.

Data Collection and Privacy Considerations

In research, a formal data collection process is necessary to ensure integrity of data and to protect against the risks of unauthorized use of research data. The primary rationale for preserving data integrity is to support the detection of errors, whether made intentionally (deliberate falsifications) or not (systemic or random errors). Equally important is the process to address the privacy and security of a research participant's identity throughout the data's lifecycle from collection and transmission, to sharing, storage, and destruction.

Risks of unauthorized use of research data are already associated with traditional data collection means and methods (i.e. via paper or local computers). However, in today's interconnected world, data is not just locked in a cabinet. Data is held by and analyzed with various methods, and transmitted across institutions over wired or wireless networks (e.g. Cellular, Bluetooth, and telephone networks) that present the risk of intercepted transmissions. These networks are susceptible to eavesdropping and wireless carrier security holes, allowing unauthorized users access to the accounts and usage data. Hackers can use hardware and technologies to intercept and decrypt calls.[2] Use of the Internet adds another complexity to security risks as investigators use cloud services and other offerings that are dependent on a multitude of third-party services such as apps or cloud providers. Such services may enhance or decrease risk, depending on several factors including the nature of the research and the method in which the data will be processed. Research teams must first be aware of these risks, then assess and mitigate them in collaboration with their institutions and IRBs.

All investigators and research staff should become familiar with their institution and/or department information security policies and procedures. Investigators should work with information security experts to review their data collection, transmission, sharing, storage, and destruction procedures to minimize the risk of unauthorized access to, or exposure of, sensitive information.[3] In IRB review, the process of protecting the privacy and security of data should be documented and methods relating to data collection, transmission, sharing, storage, and destruction should be clearly described.

To learn more about online privacy, see Glenn Greenwald's TED Talk on why privacy matters.

Below are model statements investigators may adapt to describe technology-specific risks to confidentiality or privacy.

Sample: Research Data Collection – No Guarantees Information Will Remain Confidential
There is no guarantee your information will remain confidential during collection. Your confidentiality can be protected by the protections in place on the technology being used, as well as through additional precautions suggested by the research team and other steps you can take personally. While efforts are made to protect your data, confidentiality of your data cannot be guaranteed.

Sample: Research Data Collection – Risks to Loss of Privacy
We collect information, including personal information that you voluntarily provide to us when you choose to participate in [name activity: questionnaire, survey, etc.]. When you use this interactive tool accessed through the Internet, there may be some risk(s) to your privacy. For example, we may have outside companies perform services relating to the development, operation and maintenance of this

[2] Sheldon, Robert. "Wireless Carrier Security Risks: Keeping Enterprise Data Safe."SearchMobileComputing. Apr. 2012. Web. 22 Feb. 2016. <http://searchmobilecomputing.techtarget.com/tip/Wireless-carrier-security-risks-Keeping-enterprise-data-safe>.
[3] "Introduction." *UCSF Human Research Protection Program*. Web. 6 Jan. 2016. <http://www.research.ucsf.edu/chr/Guide/chrDataSecurity.asp>.

This material is the work of the Regulatory Foundations, Ethics, and Law Program, part of the Harvard Catalyst | The Harvard Clinical and Translational Science Center. Funded by NCATS (UL1TR002541).

research website or relating to other services. These third-party service providers may have access to your personal information, as is reasonably necessary, for their services.

We take great care to protect your information; however, there is a slight risk of loss of privacy. This is a low risk because we code your data by separating your personal information (information that can directly identify you (such as your name or phone number) from the research study data. Only a few members of the research team are allowed to see your identifiable information. All others will only be able to see your coded information. The information that is obtained in connection with this study and that can be identified with you will remain confidential and will be disclosed only with your permissions or as required by law. The information collected about you will be coded using a fake name (pseudonym) for initials and numbers, for example ABC–123, etc., and the information which has you're identifiable information will be kept separately from the rest of your data.[4] However, even with removal of this information, experts in re-identification may be able to reverse our processes and /or attempt to re-identify an individual given enough cross-reference information about him or her.

Accidental public disclosure may occur such as unintended data breaches by hacking or other activities outside of the procedures authorized by the study. In such a case, your data may be misused or used for unauthorized purposes.

Sample: Research Data Collection – Protections Utilized by Study Team

The following procedures will be used to collect and protect the confidentiality of your study records [Please describe all types of electronic data]. All electronic files [include all the types of electronic files that are used, such as databases, spreadsheets, etc.] containing identifiable information will be password protected. Such files will also have password protection to prevent access by unauthorized users. Only the members of the research staff will have access to the passwords. Back-up data may be kept on server logs even after this research has been completed. At the end of this study, when investigators publish their findings, the information will be presented in summary format: you will not be identified in any publications or presentations. Data will be kept for the length of the study [list out the length of study in months or years]. After that time all identifiable data about you will be destroyed or de-identified, meaning we may retain and share certain elements of the study records for future research, but we will replace your identifying information with a code that does not directly identify you.

[4] http://oprs.usc.edu/files/2013/04/Informed-Consent-Booklet-4.4.13.pdf

This material is the work of the Regulatory Foundations, Ethics, and Law Program, part of the Harvard Catalyst | The Harvard Clinical and Translational Science Center. Funded by NCATS (UL1TR002541).

Transmission of Research Data

Investigators and IRBs may want to include language in the consent form describing how data will be transmitted. Transmission refers to data in motion from one machine or device to another. Research data may be transmitted in a variety of forms, over wired or wireless networks, using various transmission technologies or other file sharing applications, phones, and routers. Personal identifiable data of the research participant should not be transmitted (disclosed) for research purposes outside of a Covered Entity's network prior to review and approval by the IRB, IT, and others, such as research compliance.

In research, transmissions of research data must be reasonably secure both within an institution (internal) and between institutions (external). A secure transmission process should be used, even if the data is anonymous, coded, or includes non-sensitive information. For example, data should be encrypted whenever "in transit" over any public networks, such as the Internet. Unencrypted email notifications are generally not secure, except in very limited circumstances, and should not be used to share or transmit research data externally. However, many organizations may offer email encryption services that can help mitigate the risks of emailing data over the Internet. Prominent examples of unsecure transmissions include messaging via Facebook or other social media and text messages, which are stored by the telecommunications provider and therefore are not secure when transmitted.

Terms such as Secure Sockets Layer (SSL and HTTPS) or Secure File Transfer Protocol (SFTP) are indications that the data is being encrypted during transmission. Investigators should check with their IRB and institution to learn about guidance, software, and resources to encrypt files before transmission. If the investigator develops a practice for a secure data transmission process, then it is less likely a data breach will occur, although breaches, such as hacking, can occur even with the best practices in place.

Below are model statements investigators may adapt to describe data transfer.

Sample: Transmission of Research Data
By signing this informed consent, you give permission for the transfer of a copy of this data to [specify where, i.e., locked file cabinet in a locked office] located at [specify physical or virtual location, institution's network drive, etc.] at [specify individual, agency, company, affiliate, etc.]. << If sponsor will have access to the records, include: Research records may be reviewed and/or copied by the sponsor. [5] *>> [Specify individual, agency, company, affiliate, etc.] and [specify individual and/or PI at the receiving agency, company, affiliate] will be responsible for maintaining the security and confidentiality of the transferred data [specify individual, agency, company, affiliate, etc.] [Specify individual and/or PI at the receiving agency, company, affiliate] will continue to have responsibility for your research data for this research study. All original research records, both hard copy and electronic, will be maintained at the [specify individual, agency, company, affiliate, etc.] in accordance with current records retention requirements. Any information shared with [specify individual, agency, company, affiliate, etc.] may no longer be protected under the same laws as [specify individual, agency, company, affiliate, etc.].*

[5] "VA Informed Consent Form." U.S. Department of Veterans Affairs. Web. 6 Jan. 2016. <http://www.va.gov/>.

Sample: Transmission of Research Data

We are careful to ensure that the information you voluntarily provide to us is as secure as possible; however, you must be aware that transmissions over the Internet cannot be guaranteed to be completely secure.

This material is the work of the Regulatory Foundations, Ethics, and Law Program, part of the Harvard Catalyst | The Harvard Clinical and Translational Science Center. Funded by NCATS (UL1TR002541).

Online Tracking and Cookies

Investigators and IRBs may want to consider adding language to informed consents to describe online tracking and cookies. The web includes elements that may not be evident to the average user, such as tracking cookies or web beacons. Connections between a site visited and third-party services are not always obvious (e.g., as a user moves from one site to another, third parties may "watch" the activity to collect marketing research important to their clients' business). In fact, some people may be unaware that many third-party sites sometimes have the ability to monitor and track our activity on the sites we visit. This is rarely transparent to users, despite the fact that it may carry privacy risks to them. The challenge is how to communicate this to participants, many of whom will lack understanding of how relationships among various online sites work. It is important to explain those risks as clearly as possible to research participants. (To learn more, watch former Mozilla CEO Gary Kovacs's TED talk about exposing online tracking).

When browsing the web, the browser retains certain pieces of information, such as a history of the sites visited (also known as 'tracking'). Tracking is often accomplished with "cookies," small files that are stored on the user's computer and hold a modest amount of data specific to a particular website and the device used to access it. These files can be accessed either by that online service or that device itself. Cookies allow the online service to deliver an experience to a particular user (e.g., remembering the kinds of books or music a user enjoys), or enable a site to sustain information from one visit or site to the next (e.g., maintaining a 'shopping cart' for items previously put in that cart, but not yet purchased).[6]

Some cookies are temporary only, and are deleted when the browser is closed. These "session cookies" are commonly used to keep a user logged in to their online account as s/he navigates within the site. Other cookies persist indefinitely and may track the user's browsing behavior across sites or provide customization, such as remembering preferred page layout on a particular site. Familiar experiences based on persistent cookies include websites welcoming users back by name or sites displaying advertisements drawn from other sites visited.[7]

Investigators and IRBs should consider privacy risks created by tracking technologies and recommend suitable privacy safeguards before directing participants to online research data collection sites. Such safeguards may include browser privacy settings or comprehensive anonymization mechanisms.[8] https://www.privacylaws.com/Publications/enews/International-E-news/Dates/2012/6/No-need-of-informed-consent-for-authentication-and-session-ID-cookies/Most web browsers offer privacy settings designed to enable "Do Not Track" and/or "Private Browsing". Such settings will not make the participant entirely anonymous, however, as their Internet service provider (ISP), employer network, or the individual websites themselves can still track what pages that they visit.

Below is a model statement investigators may adapt to describe online tracking and cookies for web interactions.

Sample: Online Tracking

Although every reasonable effort has been taken, privacy and anonymity during Internet interactions cannot be guaranteed. It is possible that additional information beyond that collected for research

[6] "Cookies." What Are Cookies. Web. 6 Jan. 2016. <http://www.whatarecookies.com/>.
7 "Publications." PLB News. Web. 22 Feb. 2016.
[8] "Publications." PLB News. Web. 22 Feb. 2016.

This material is the work of the Regulatory Foundations, Ethics, and Law Program, part of the Harvard Catalyst | The Harvard Clinical and Translational Science Center. Funded by NCATS (UL1TR002541).

purposes may be captured and used by others not associated with this study. The web includes elements that are not always evident, including online tracking mechanisms. As you move from one site to another, third parties not involved in this research, may "watch" your online activity, including your visit to our research site. That third party may employ security and privacy policies different than ours, over which we have no control.

<<We can provide some recommended tools and practices to prevent online tracking mechanisms and improve your online privacy. For practices, first check your web browser's privacy settings to enable "Do Not Track" and/or "Private Browsing." Please note such settings will not make you entirely anonymous however as your Internet Service Provider (ISP) or employer network can still track what pages you visit. For tools, we recommend XYZ>> (Only include this sentence if you or your institution has tools and practices to share with the research participant. For recommendations on how to improve online privacy go to: privacyrights.org/online-privacy-using-internet-safely).

This material is the work of the Regulatory Foundations, Ethics, and Law Program, part of the Harvard Catalyst | The Harvard Clinical and Translational Science Center. Funded by NCATS (UL1TR002541).

Storage and Archiving including Cloud, Back-ups, and Access

In the consent form and as part of the informed consent process, investigators should inform participants (1) how research data about participants will be stored, (2) the duration of data storage, and (3) what happens to any identifying information. If applicable, describe how research data will be stored and/or with whom data will be shared beyond the end of the study. Your IRB may have a preference as to whether you must explicitly list in the consent the location where data will be stored, such as "in the cloud," or may use broader language such as "on local servers." Some IRBs may prefer to emphasize how the data is protected versus specifying storage location. Check with your IRB to understand their preference.

Some investigators use consumer-based cloud storage solutions to remotely store and exchange files with collaborators. Broadly defined, cloud computing refers to third party-hosted computing services that are accessible over the Internet.[9] Popular services include Dropbox and Amazon Cloud, among many others. The cloud can be used for research and provide closed or open access to data.

Most cloud services and apps were not designed with research regulatory compliance or human subject protection ethics or considerations in mind. In many cases, free services offered by cloud providers are not compliant with regulatory requirements such as HIPAA. However, these same providers may have a more secure fee-for-service model that provides adequate coverage. For example, Dropbox can be made HIPAA-compliant within their paid service model and with appropriate changes. It is important for investigators to be familiar with the differences in service tiers for the technology they choose to employ. Check with your institution to inquire about specific pre-approved solutions, or whether there is a process to obtain approval and secure compliance.

Contracting adds additional concerns that make using cloud storage for research data difficult for investigators to navigate. Cloud services ordinarily have non-negotiable end-user license agreements with inflexible terms of use and/or data ownership clauses that may conflict with the research.

IRBs often do not have the expertise to evaluate cloud services, and so IRBs often require sign off from others. An ancillary review should be conducted to *determine whether the cloud service is suitable for use in research in light of any regulations like HIPAA and other data privacy laws. If the investigator decides to use a specific cloud service, it* should be fully understood and may need to be approved by the IT Department and the IRB for use in research. The investigator should seek IRB, IT, and security expertise to identify and implement appropriate supplemental privacy and security safeguards into the protocol or research project.[10] Remember, users must follow rules dictated by the terms of use. Many institutions own their "own cloud" and do not negotiate for outside third-party services. If, however, a third-party cloud service is offered through your institution or employer, many of the rules may have been negotiated but not necessarily for research purposes. Please be sure to ask.

Below are model statements investigators may adapt to describe storage and archiving of data. (Please see the devices/apps section for language on data stored on remote device platforms).

[9] "Harvard Catalyst Guide to Technologies Used in Research." *Harvard Catalyst*. Web. 6 Jan. 2016. <https://catalyst.harvard.edu/pdf/regulatory/Investigators Guide to RDM practice.pdf>.

Sample: Cloud Repository

Investigators will store your data in a controlled-access repository in the cloud. The repository is controlled-access, meaning only certain research team members have authorized accounts to access the data. "In the cloud" refers to servers in a data center that are managed by a third party and accessible through the Internet. Any computing device with access to the Internet could connect to this closed-access repository. We use [X, Y, Z] methods to protect data and methods to ensure data will be used for the approved purpose.

Sample: Cloud Storage

Your study data will be stored in the cloud. "In the cloud" refers to servers in a data center that are managed by a third party and accessible through the Internet. When storing your study data, we will replace your name with a random code on all your study data. The coded data will be encrypted and stored on a secure cloud server under the control of [XX] to prevent improper access.

Sample: Archiving Computer Data

Archiving means saving for use at a later date. Computer data, such as instant messaging files, captured web site records, and copies of electronic mail will be archived. This data will be stored in password-protected files on a computer in [LOCATION]. Archived computer data will be also stored <<insert location>> and locked in a filing cabinet in a secure [LOCATION] with access limited to authorized individuals.

Research Data Destruction

Research data destruction isn't simply deleting the data. Devices are becoming harder to destroy and data are routinely recovered from devices that have been burned, crushed, submerged in water, or dropped from great heights. Additional steps must be taken to sufficiently destroy data so the data cannot be recreated, reconstructed, or extracted. This can be done through techniques and technologies specifically designed to make the data destruction irreversible. Common methods for data destruction include overwriting (requires overwriting software), degaussing (requires a device called a Degausser, that removes the magnetic field of the storage device), and physical destruction (e.g., disk shredding). The choice of destruction methodology should be based on the risk posed by the sensitivity of the data being destroyed and the potential impact of unauthorized disclosure.

Reference data retention policies for the minimum period of time the research funder and your institution requires you to maintain data. Review other relevant institutional and publication requirements, as well as guidelines for data retention and destruction. Data collected in a federal- or state-funded project may require public access to data, which may result in specific requirements for how, when, and what data is destroyed. For example, if data contains PII about research subjects and a separate de-identified data set has been created, there may be an obligation to destroy the data containing the identifiers.

For data obtained through an agreement with an outside provider or institution, you may be required to return the data at the end of the project, or to destroy the data and document that you have done so. As data becomes more available and linked across many devices, both mobile and fixed, the challenge of a complete destruction of all possible copies and backup of the data is exponentially increased. The research team should be aware of every location for the study-associated data and its back-up location. Documentation of research data should be kept up to date to attest the full data set is accounted for and destroyed from all locations. When documenting research data, include: source of data, size of data set, number of records, variables, format of data, and final disposition of data.

Below is a model statement investigators may adapt to describe research data destruction.

Sample: Research Data Destruction
Data will be kept for the length of the study [list out the length of study in months or years]. All original research records, both hard copy and electronic, will be maintained at the [specify individual, agency, company, affiliate, etc.] in accordance with current records retention requirements. We will destroy research data kept on backups, but we may not able to destroy data that was saved on the institution's server logs even after this research has been completed.

Any information shared with [specify individual, agency, company, affiliate, etc.] may no longer be protected under federal law. We will destroy your research data at the end of the study, meaning we will not retain your information in coded or other form. However, we may not be able to destroy research records that were transmitted or copied by [specify individual, agency, company, affiliate, etc.]. The [specify individual and/or PI at the receiving agency, company, affiliate] will be responsible for maintaining the security and confidentiality of the transferred data [specify individual, agency, company, affiliate, etc.].

This material is the work of the Regulatory Foundations, Ethics, and Law Program, part of the Harvard Catalyst | The Harvard Clinical and Translational Science Center. Funded by NCATS (UL1TR002541).

Electronic Informed Consent

Electronic Informed Consent (e-Consent) is an evolving platform for consenting research participants, either on-site or remotely, using a computer-based consent process. As with traditional paper-based informed consent, e-Consent is not only a form, it's also a process. Any e-Consent process conducted on-site or remotely should include an opportunity for subjects to ask questions and receive answers prior to providing their consent to participate in the study. The consent process can be implemented on a number of electronic systems such as computers, tablets, and phones. These platforms may also use multiple media types (e.g., text, graphics, audio, video, podcasts, and interactive web sites, biological recognition devices, and card readers, etc.) to convey information related to the study and to obtain documented informed consent.[11] Additional considerations should include the process to validate identity and how the consent form will be signed electronically (e.g., Adobe e-sign). Investigators must receive IRB approval for the e-Consent process, even if they already have IRB approval for a paper version of the consent process.

Below are model statements investigators may adapt to describe the technology-specific risks in e-Consent.

Sample: Reading the Informed Consent

On the next screens, you will view the informed consent document. Please read all sections of the informed consent document. After each section, you may be asked to answer some questions before continuing onto the next section. After you have read all sections, you will be given the opportunity to go back and review all sections.

Swipe the screen from bottom to top with your finger to scroll through each section of the informed consent document. When you reach the end of a section, you will be able to touch the Continue button.

If there is a word or group of words that you do not understand, touch and hold your finger on the word until a small box appears, then tap the "unfamiliar term" selection. This will highlight the word and allow your physician to explain the meaning to you during your discussion.

Please touch the "Continue" button below to read the informed consent document.

[11] "Use of Electronic Informed Consent in Clinical Investigations." *Fda.gov*. Web. 6 Jan. 2016. <http://www.fda.gov/downloads/Drugs/GuidanceComplianceRegulatoryInformation/Guidances/UCM436811.pdf>.

Email

Email is a communication tool; there are many email service companies such as Gmail, Microsoft Outlook, Yahoo!, and many others.

Investigators and the IRB should determine whether the email service is suitable for use in research in reference to regulations such as HIPAA and other data privacy laws. While employers provide email for employees, investigators should determine if the office email is an appropriate tool for communication with research participants. For example, email encryption may be essential to protect a research participant's protected health information.[1] If a non-employee email service, such as a third-party email service is used, keep in mind that each email service company has its own terms of use agreement and privacy policies. Users must follow rules dictated by the terms of use, some of which are common sense while others are based on the company's specific policies.

Investigators and the IRB should take into account that communicating with a research participant via email could lead to possible problems in interpretation of both questions and responses. The research participant will be unable to read visual and auditory cues, such as facial expressions and voice intonation, which are often used to convey and/or emphasize meaning. Thus, investigators may need to ask explicit clarifying questions to accurately interpret responses and provide additional information to ensure potential participants understand the questions and information being communicated.

Below are model statements investigators may adapt to describe email.[12]

Sample: Email
There is no guarantee your email information will remain confidential. Your confidentiality can be protected by the protections in place on the technology being used and additional precautions suggested by the research team. While efforts are made to protect your data, confidentiality of your data cannot be guaranteed.

The technology you use to write and send your email(s) can increase the protection of your information. For example, you can use a strong password, anti-virus and anti-malware protections, and a secure wireless network.

The research team will work with you on how to increase your security when using email. They will explain steps you can take including how to encrypt your emails, what information you should avoid including in your emails, and warnings to watch for (e.g. emails from unknown users, or emails asking for more information than the research team explained you would be asked to share). If you receive a suspicious email, contact the research team immediately.

When sending emails, make sure to limit the personal information you include, such as your full name, address, social security number, and other personal information. An email account can be hacked by an unauthorized user. There is a risk your emails could be read or altered by unintended recipients. Although it is unlikely that someone will try to gain access to your email, since email is sent over a wireless network, there's a risk it may be intercepted. To decrease this risk, always choose to send emails over a secure wireless network.

[12] "Internet Based Research." *University of California*. Web. 6 Jan. 2016. <http://cphs.berkeley.edu/internet_research.pdf>.

This material is the work of the Regulatory Foundations, Ethics, and Law Program, part of the Harvard Catalyst | The Harvard Clinical and Translational Science Center. Funded by NCATS (UL1TR002541).

If you have concerns about using an established email, you can establish a new email account (making sure to not include your name). It is easy to start a free webmail account *[include link to suggested webmail signup, such as Gmail] completely for this purpose.*[13]

Sample: Email - encryption

Email notifications are generally not secure, except in very limited circumstances, and should not be used to share or transmit research data. For this study, data will be encrypted when "in-transit," or while being moved in the network to the secure storage location.

[13] "Encryption Guide: Drugs on Forums Project." *Curtin University: NDRI*. Web. 6 Jan. 2016. <http://ndri.curtin.edu.au/drugsonforums/encryption.cfm>.

Mobile Health: Devices and Apps

Mobile Health (mHealth) is the method of delivering healthcare through mobile technology. mHealth can include mobile devices and apps (e.g. laptop, tablet, iPhone, Android) and wearable technology (e.g. Fitbit). The use of mobile technologies allows investigators to collect data from the research participant when s/he is not physically present at the doctor's office. This allows for a dramatic increase in data collection to aid researchers in understanding the illness or disease being studied.

A mobile device is a computing device that can easily be carried or moved, such as a smartphone, tablet computer, portable hard drive (e.g., flash drives, USB memory sticks, or similar storage devices). These devices are particularly susceptible to loss or theft. If mobile devices are used for initial collection of subject identifiers, investigators must encrypt subject data files. Investigators should consider using a device that can be wiped remotely in the event of loss or theft.[14]

A mobile app is a software program that can be downloaded to a device. The data the app collects can be stored locally to the device or sent to remote storage locations. Mobile apps can collect data through two different mechanisms: passive and active data collection. In passive data collection, the participant has little awareness of the data collection effort, which requires no explicit actions on the participant's part. Active data collection involves explicitly asking participants for information, preferences, and opinions.

Investigators should work with IT and the IRB on mechanisms to secure data obtained using mobile technologies. Data may be secured by a number of means such as app password protection, or encrypted data transmission and storage. Each mechanism must comply with institutional policies and protect the individual using the app. Investigators should notify the IRB if the app is commercially available or is being developed. For commercially available apps, investigators should reach out to the appropriate research/compliance office (e.g., Office of Research, Research Administration, etc.) as a Data Use Agreement or contract may be required. Whether the app is custom or commercial, the investigator should inform the participant of the type of data being collected, and the method of collection. Investigators may not collect other forms of data (e.g. location information) unless it is explicitly stated in the consent form. The consent form should provide enough details about the mobile device and app, as well as the potential risks, to allow the research participant to make an informed decision about participation.

Below are model statements investigators may adapt to describe mobile devices and apps.

Sample: Downloading Apps
If you decide to join the study you will need to download the study application on your mobile phone. Then, periodically we will ask you to answer questions and perform some tasks via your mobile phone. These tasks may include answering questions about your health, exercise, medicines, and additional surveys, as well as performing some brief activities while holding your phone. Your study data will include your responses to surveys and the measurements from the phone itself when you perform a task. Tasks can include [insert tasks].

[14] "Special Considerations in IRB Review." *University of Notre Dame*. Web. 6 Jan. 2016. <http://or.nd.edu/research-compliance/human-subjects-research/irb-procedures-manual-guidelines/special-considerations-in-irb-review/>.

This material is the work of the Regulatory Foundations, Ethics, and Law Program, part of the Harvard Catalyst | The Harvard Clinical and Translational Science Center. Funded by NCATS (UL1TR002541).

Your data, without your name, will be added to the data of other study participants and made available to groups of certified investigators for analysis. You also will have a unique account that you can use to review your data on the study website.

PROCEDURES**: **What will you be asked to do?
***Download a mobile app (free) and register an account:** You need to have the study app on your phone in order to participate in this study. Everyone who enrolls will first complete an electronic registration process. The registration process can be done through the study app or the study web portal. Registration will include entering your name, email address, and other general information about yourself. As part of this process you will also confirm your agreement to participate in the study.*

***Tasks**: We will ask you to perform specific tasks while holding or using your mobile phone. Examples of such tasks are:*

- *[insert bulleted list of tasks]*

These tasks should take you about [insert number] minutes each week. We will send notifications on your phone asking you to complete these tasks and surveys. You may choose to act at your convenience, (either then or later) and you may choose to participate in all or only in some parts of the study. You have the right to refuse to answer particular questions or participate in particular aspects of the study.

Sample: General Risks
The use of technology as part of this research project can present risk(s). Generally, it is possible that private data from a mobile device may be intercepted during transmission. [Describe how data is or will be transferred/transmitted. Indicate what level of encryption will be used, if any. Describe to what extent that any identifiers will be removed]. It is also possible that your data could be accessed by others should the participant lose his or her mobile device or lend the device to other people. Some additional risks are related to a loss of confidentiality, especially when using electronic devices to transmit, store, and access data. There is some possibility that others may see your open webpage or smartphone communications. In addition, certain apps or app protections may affect the battery life of the device [this needs to be disclosed to participants/included in the protocol]. Measures to protect security in these instances are described below. Any known potential loss of confidentiality will be disclosed here.[15]

Sample: App or Device Security Protections
It is highly recommended that you set up a passcode on your own phone and/or electronic device to help prevent unauthorized access to your device and research data, especially for studies that involve collection of any private health information. It's also recommended that a remote disable feature be set up on your device in case it's lost or stolen. This will allow you to remotely disable or remove any apps and/or data. [Describe any protections being offered to participants so they can protect or encrypt data on the device or through the app itself].

Sample: Limits to Data Protections or Confidentiality
In order to get access to intended or target data, the investigator might happen to get access to or be unable to avoid seeing certain data. While the investigator might have gained access to your location

[15] "Consent Form to Take Part in a Mobile/Electronic Device or Technology Study." Rutgers University. Web. 6 Jan. 2016. <http://comminfo.rutgers.edu/~cgal/IRB.pdf>.

data, or financial, or other personal information on your device, this data will not be recorded or retained. Instead, we will only extract data that has already been stated in previous paragraphs.

Sample: Data Transmission and Storage on Electronic Devices
Research data will be sent from the electronic device [or mobile app] to the research team via [Describe how data will be transmitted. If the data will be on paper forms, describe how they will be sent to the investigator. If data will be stored electronically on a server, describe which server/where and security methods to maintain privacy]. Please note that we will keep this information confidential by limiting individual access to the research data and keeping it in a secure location. The research data will be stored [MUST list out all secure storage/maintenance of the data, e.g., password-protected computers, encryption methods etc.].[16]

Sample: Risks, Discomforts and Inconveniences Using Mobile Apps
Other people may glimpse the study notifications and/or reminders on your phone and realize you are enrolled in this study. This can make some people feel self-conscious. You can avoid that by putting a passcode on your phone to block unauthorized users from accessing your phone content.

Be safe – just as you would not text while driving, do not fulfill study tasks while driving. Wait until you are in a safe place to perform tasks!

You may have concerns about data security, privacy, and confidentiality. We take great care to protect your information, however there is a slight risk of loss of confidentiality. This is a low risk because we work to protect your privacy by separating your personal information (information that can directly identify you, such as your name or phone number) from the research data. However, even with removal of this information, it is sometimes possible to re-identify an individual given enough cross-referenced information about him or her. This risk, while very low, should still be contemplated prior to enrolling.

Data collected in this study will count against your existing mobile data plan. You may configure the application to only use wi-fi connections to limit the impact this data collection has on your data plan. <<[Investigators should only include this language if the technology has been equipped to only use wi-fi connections. Please check with IT to ensure the technology has been set-up to do so before including in the consent form]>> You can respond to the surveys via the web portal instead of via your mobile phone, but all the tasks must be completed using your mobile phone.

Sample: Costs
There is no cost to you to participate in this study other than costs related to your mobile data plan, if applicable.

Sample: Confidentiality
Your confidentiality will be kept to the degree permitted by the technology being used. No guarantees can be made regarding the interception of data sent via the Internet by any third parties.

Sample: Lost of Stolen Mobile Device
<<Depending on who owns the device (research participant or research study)>> Remote data deletion will be performed in the event of a lost or stolen phone [insert who will be responsible for wiping the device and indicate a timeline in which the deletion will be completed]. <<[Investigators should only

[16] "Consent Form to Take Part in a Mobile/Electronic Device or Technology Study." Rutgers University. Web. 6 Jan. 2016. <http://comminfo.rutgers.edu/~cgal/IRB.pdf>.

This material is the work of the Regulatory Foundations, Ethics, and Law Program, part of the Harvard Catalyst | The Harvard Clinical and Translational Science Center. Funded by NCATS (UL1TR002541).

include this language if the technology has been equipped to remove data remotely. Please check with IT to ensure the technology has been set up to do so before including in the consent form]>>.

Sample: Information Stored in Medical Record

The information about you gathered from the mobile device or app [will or will not] be stored in your medical record history. Your primary care physician and other medical professionals to [will or will not] be able to view the information you shared and that was collected about you during your participation in this study.

Sample: Secondary Use of Data

The mobile application company chosen for this research study may have access to your information and use it in other ways. There is also the chance that depending on the agreement the research team and the mobile application company established, the mobile application company may own some or all of your information.

Mobile Health: Wearables

Mobile Health (mHealth) is the method of delivering healthcare through mobile technology. mHealth can include mobile devices and apps (e.g. laptop, tablet, iPhone, Android) and wearable technology (e.g. Fitbit). The use of mobile technologies allows investigators to collect data from the research participant when s/he is not physically present at the doctor's office. This allows for a dramatic increase in data collection to aid researchers in understanding the illness or disease being studied.

Wearables are worn technologies that have sensors built in. These sensors can connect to the web (e.g., wi-fi) or be plugged into a computer to track information. A majority of wearables have smart technology capabilities. Smart technology is a device or system that has advanced technology allowing it to be connected to the Internet and used interactively. Examples of common wearables include fitness trackers, smart watches, smart clothing, sport watches, etc. Wearables can track movement, distance, and speed using GPS, accelerometers, and gyroscopes. Additionally, once in contact with skin, wearables can record body functions such as heart rate, perspiration, temperature, and muscle activity.

While wearables are not generally used to diagnose medical conditions or illnesses, they are often used to track the activity of a research participant. This technology is seen to decrease the burden on a research participant who would typically track their activities in a journal or diary. It can also allow for the collection of additional research data such as heart rate, temperature, body fat composition etc., without the use of separate medical equipment. Additionally, the activity recorded by the wearable can often be seen by the investigator in real time, through an online system.

Research using wearables is subject to the same regulations and ethical norms as a traditional paper-based data collection. That said, wearables raise unique concerns regarding the ease and real time nature of the data collection, as well as concerns regarding third party access to the data. Investigators must take care to clearly inform research participants about these concerns and any relevant risks.

Below are model statements investigators may adapt to describe wearables.

Sample: Activity Monitor
This device does not pose any medical risk and does not diagnose any medical conditions or illnesses. Wearing the activity monitor may cause minimal discomfort. The device is small, weighing only a few ounces, and can be easily worn on the torso by attaching it to a belt or waistband, pants, shirt, or undergarment.

Sample: Physical Activity Monitor
You will be given a physical activity monitor called a "[insert name of the product]" with instructions on how to use the device. The device will be worn as a [insert how the device will be worn, e.g., wristband], and it will record [insert what the device will record, e.g., your levels of physical activity during the day and will record the number of hours you sleep each night]. You will be asked to use this device for [list out the amount of time] and will be taught how to follow your physical activity levels [insert location where the activity levels can be view, e.g., Fitbit website]. The website will also help you keep track of your dietary intake (types and amounts of food you eat) types of physical activity (exercise) that you do and heart health factors such as weight, heart rate, blood pressure, and blood sugar.

The [insert name of the product] activity monitor is an item you can buy in a store, and it is not painful

This material is the work of the Regulatory Foundations, Ethics, and Law Program, part of the Harvard Catalyst | The Harvard Clinical and Translational Science Center. Funded by NCATS (UL1TR002541).

to wear this plastic monitor around [insert location the device will be worn]. [Insert any problems that may arise while wearing the device, e.g., you may feel a little skin irritation or itching if the monitor is worn too tightly around the wrist or you may hear a ticking noise while wearing the device].

Sample: Risks

There is also the possibility of minor skin irritation associated with wearable devices. We recommend taking it off occasionally, not wearing it too tightly, and keeping it clean and dry. You should regularly clean your wearable device—especially after working out or sweating. Rinse the wearable device with water or wipe it with a small amount of rubbing alcohol. Do NOT use hand soap, body soap, dish soap, or household cleaners which could get trapped beneath the band and irritate skin. Always dry the wearable device well before putting it back on. If you start to experience skin irritation on your wrist, we suggest you remove the device and contact a member of the study team to discuss the issue and determine whether you would like to continue participating in the study.

Sample: Wearable Confidentiality

To ensure your confidentiality while wearing the [insert the name of the wearable device] to the extent permitted by law, the following measures will be taken:

- *You will be assigned a unique identifier code and all the information you provide will be listed under your code.*
- *There will be only one hard copy with your name/identity and all information [questionnaires, surveys, etc.] will be stored in a secure filing [room, cabinet, etc.]. This [room, cabinet, etc.] can only be accessed by the [PI, co-investigators, research coordinators, etc.].*
- *There will only be one file maintained on a password-protected server. This file can only be accessed by the [PI, co-investigators, research coordinators, etc.].*
- *The de-identified data will be kept [insert period of time], which could mean till the end of the study, even after you have completed your part. If the results of the study are published, your identity will remain confidential.*
- *The company that manufactures the wearable will have access to your data, but they will not have access to your identity because coded identification (ID) numbers will be used rather than names. Your data would be anonymous to the manufacturing company [if available, list out manufacturing company name]. [If applicable: Please talk with the research staff about how your information may be shared with the company]*
- *[insert any additional measures that will be taken]*

Sample: Privacy and Confidentiality for Wearable that Uploads Data to a Website

Study participants' data collected from the [insert name of the product] website will be downloaded weekly by the research study database manager. This data will be entered into the study database under the participants' study identification number. Depending on the language in the Business Associates Agreement, [insert name of the product] may have access to your data. The research study staff have developed an agreement to uphold the privacy standards set by the Health Insurance Portability and Accountability Act (HIPAA), protecting information that is directly linked to you (e.g., name, address, social security number, etc.).

Sample: Fitbit

Because the Fitbit software requires regular access to a computer with Internet or a smartphone, you also must have regular access to one of these devices to participate. You cannot participate in the study if you have injuries or health conditions that prevent you from safely participating in physical activity.

You will receive instructions on how to use the Fitbit and guidelines for how to upload the data into the associated software/app. You will be provided with a study-specific username and password to be used with the Fitbit software/app throughout the duration of the study. As such, members of the study team will have access to any data you choose to enter into your Fitbit profile (e.g. diet, social media, etc.). You are encouraged to use the software/app frequently to help you monitor your progress towards increasing your physical activity. Your physical activity behaviors will be monitored by a member of the study team using Fitbit data collected via a 3rd party software company. This information is critical for helping our team to understand your current lifestyle habits with regard to physical activity and will not contain any personally identifiable information about you. This data will be used for analysis in our research project and will not be shared with anyone else.

Sample: Apple Health Kit

You have the options to contribute activity data collected through:

- *The sensor on your iPhone or any wearable activity device (e.g. Fitbit, Jawbone, etc.).*
- *Other applications and data available through Apple Health Kit.*

You can choose not to provide this data and still participate in the study. We will NOT access your personal contacts, other applications, personal photos, and text or email message.

Sample: Wearable Computers (e.g., Google Glass)

You are being invited to participate in a voluntary research study using a technology, a wearable computer that can transmit data such as video and still images.

If you choose to participate, the doctor who examines you will wear <<[insert name of wearable computer]>> while they care for you. They will videotape your physical exam and take any relevant pictures. The video and pictures will then be uploaded to a secure server where a more experienced doctor can see them. You could benefit from this, as the information provided may help the more experienced doctor make decisions about your medical care.[17]

[17] "Informed Consent Form." *University at Albany*. Web. 6 Jan. 2016. <http://www.albany.edu/orrc/irb-forms.php>.

Online Survey Tools

Investigators may utilize online surveys or questionnaires to gather data from many participants in a short amount of time. There are a wide variety of online tools available for online surveys. Use of third-party survey software companies such as SurveyMonkey, Psychsurveys.org, Mechanical Turk, Zoomerang, Lime, and others may be permitted for most minimal risk studies that employ online survey procedures. However, it is important to note that third party survey software companies differ from survey tools made available through academic institutions (e.g., Qualtrics or REDCap). For example, when using a third party to administer surveys, the website might store collected data on their own company backups or server logs which may be kept beyond the timeframe of the research project. The investigator should be aware of the conditions and terms of the survey company's storage and retention policy, and include relevant information in the protocol or other documents submitted to the IRB, including the consent information provided to participants. Investigators should check with their institution's IRB and/or IT department for a list of vetted online survey tools.

Data security requirements for projects that include online surveys or questionnaires will depend on the design and complexity of the project and the specific study population. Some factors for consideration include: a) whether it is a one-time survey or a longitudinal study with follow-up; b) whether participants will be able to stop and re-enter the survey(s); c) whether data will be collected to facilitate a remuneration process; and d) whether minors are included as a population and, if so, any applicable parental permission considerations. If security measures are not adequate to protect the data being collected (e.g., the risk/benefit ratio is too high), use of the given survey company may not be approved.

Few surveys are truly anonymous. Even though a participant may not be asked for his/her name in the survey, other pieces of information (IP address, email address, zip code, etc.) and/or demographic questions (sex and race, especially in a small sample with low diversity) can potentially be used to glean the identity of individual participants. As part of the consent process, prior to participation research participants need to be informed of these concerns and all data security measures that will be taken.[18]

Below are model statements investigators may adapt to describe online survey tools.

Sample: Participating in an Online Survey
If you agree to be part of the research study, you will be asked to complete a computer survey that asks you to [describe in detail what you want the participant to do]. We expect this survey to take [enter the number of minutes] minutes to complete.

Investigators will not be able to link your survey/interview responses to you, but they will know that you participated in the research if you provide your contact information. We plan to publish the results of this study, but will not include any information that would identify you.

You may choose to not answer an individual question, or you may skip any section of the survey by skipping the question or clicking "Next" at the bottom of each survey page to move to the next question.[19]

[18] "Internet Based Research." *University of California*. Web. 6 Jan. 2016. <http://cphs.berkeley.edu/internet_research.pdf>.
"Forms & Templates." *UMassAmherst*. Web. 6 Jan. 2016. <https://www.umass.edu/research/compliance/human-subjects-irb/forms>.

[19] "Institutional Review Board (IRB)." *Lawrence Technological University*. Web. 6 Jan. 2016. <http://www.ltu.edu/provosts_office/irb.asp>.

Sample: Coded Responses

Your survey responses will be coded so that the research staff will not be able to link your responses back to you. When completing the survey, your responses will only be saved to the survey software and accessible for the research staff to view after you hit "submit." Only authorized research staff will be given access to the survey data, but since the survey software is located on the Internet there is a risk it could be hacked into by unauthorized users. To further protect your survey information, make sure to use a strong password into the survey software system and to not share that password with anyone. <<If applicable, the survey includes a section at the end for you to include your personal contact information for the research staff to contact you for further information. If you are concerned about your identity being found out, please talk to the research staff on ways to protect your survey information.>>.[20]

Sample: Participating in a Survey – Provide Email Address

If you wish to participate in this research, please follow this link and fill out a survey: [Insert URL here]. The survey will take you [ex.15-20 minutes] to complete.

At the end of the survey, you will be asked to provide your email address. Your response is confidential, and your colleagues' responses are anonymous. After we finish collecting data and make sure your response is matched with your raters' responses, your email address will be deleted from the data.

Sample: Participating in a Survey – I agree/I do not agree

Please retain (print) a copy of this form for your records. If you are 18 years of age or older, understand the statements above, and will consent to participate in the study, click on the "I Agree" button to begin the survey/experiment. If you do not wish to participate in this study, please click the "I Do Not Agree" button to exit this program.[21]

Sample: Research Electronic Data Capture (REDCap)

This study will collect data in Research Electronic Data Capture (REDCap). REDCap was developed specifically around HIPAA-Security guidelines and is implemented and maintained according to [Institution Name] guidelines. REDCap currently supports > 500 academic/non-profit consortium partners on six continents and 38,800 research end-users. REDCap servers are securely housed in an on-site limited access data center managed by [name of institution's department here (e.g. divisions of biostatics)]. All web-based information transmission is encrypted. The data is all stored on a private, firewall- protected network. All users are given individual usernames ids and passwords, and their access is restricted on a role-specific basis. [22]

Sample: Survey Monkey and the US Patriot Act

Please note that the online survey is hosted by Survey Monkey, which is a web survey company located in the USA. All responses to the survey will be stored and accessed in the USA. This company is subject to U.S. Laws, in particular, to the US Patriot Act/Domestic Security Enhancement Act allowing authorities to access records with your responses stored and accessed in the USA. The security and privacy policy for Survey Monkey can be viewed at: surveymonkey.com/mp/policy/privacy-policy /. **[23]**

---

[20] "Privacy Policy." *SurveyMonkey*. Web. 5 May 2016 <*https://www.surveymonkey.com/mp/policy/privacy-policy/*>.

[21] "Consent Form to Take Part in a Mobile/Electronic Device or Technology Study." Rutgers University. Web. 6 Jan. 2016. <http://comminfo.rutgers.edu/~cgal/IRB.pdf>.

22 "Boilerplate Language for Inclusion in Grants and IRB Documentation." WUSM REDCap. Web. 13 Apr. 2016. <http://www.biostat.wustl.edu/redcap/?page_id=242>.

23 Considerations and Recommendations Concerning Internet Research and Human Subjects Research Regulations, with Revisions. SACHRP, 13 Mar. 2013. PDF.

This material is the work of the Regulatory Foundations, Ethics, and Law Program, part of the Harvard Catalyst | The Harvard Clinical and Translational Science Center. Funded by NCATS (UL1TR002541).

Social Media

Social networking has changed the way we interact with friends and associates. Social networks such as Facebook, Twitter, YouTube, and Google+, play a significant role in our lives. Social media can be defined as any online and mobile resource that provides a forum for generating, sharing, or discussing ideas and content. Specific applications and web tools, many of which are free, are based on different, sometimes overlapping, themes and purposes, variably grouped as online communities (e.g., patient support groups, population-specific dating services); social networking (e.g., Facebook; Twitter); professional networking (e.g. LinkedIn); content production and sharing (e.g., YouTube, Tumblr, blogs); location-based services (e.g. Tinder, Grindr); and others. Many social media web services contain one or more platforms that allow users to view one another's networks and interact with one another in real time. These include comment spaces, chat rooms, discussion forums, and the like. [24]

In research, social media is most often used for recruitment. This method of recruitment is subject to the same regulatory and ethical norms as traditional recruitment, including the requirements of prospective review and approval, compliance with applicable federal and state laws, fair and equitable subject selection, respect for the privacy and other interests of potential participants, and sensitivity to the norms and values of different communities. That said, social media recruitment raises unique issues, including the ease with which personal health information can be accessed via these sites. For these reasons, greater care may be required to ensure participants are adequately informed of privacy risks.

Social media may also be used as a venue for participants to communicate with study staff and/or other participants. This carries several risks, including the risk that participants will be un-blinded because of someone's description of their experience in the trial, and the risk of participants posting misleading information that undermines participant understanding of the study. Efforts should be made to inform participants of these risks and educate them on the importance of appropriate online communication while enrolled in the study.

To learn more about ways to protect yourself on social networks see: staysafeonline.org/stay-safe-online/protect-your-personal-information/social-networks.

Below are model statements investigators may adapt to describe social media recruitment.

Sample: Facebook App

Facebook will have access to the information collected through the app. In addition, Facebook will have access to any information that we provide to you using this app. You should also know that your individual Facebook privacy settings will determine who can see the app in your profile, your posts regarding the app, and if you invite your Facebook friends to participate. Your participation in the study may be made public. Facebook may reveal or confirm that you have participated in the study based on their policies and practices.

[24] "The Use of Social Media in Recruitment to Clinical Trials: A Guide for Investigators and IRBs." *Harvard University: Petrie-Flom*. Web. 6 Jan. 2016. <http://petrieflom.law.harvard.edu/assets/publications/PFCannualreport12_13.pdf>.

Video, Audio, and Photography Recordings

Investigators may choose to use video (moving picture), audio (sound), or photograph (image) to record information for research. Methods of recording research participants can include use of a camera, camcorder, smartphone, voice note, Skype, Adobe Connect, etc.

Recording the voice and/or image of an individual creates a distinct type of record that requires unique handling and storage, as well as consent. Investigators need to be mindful of the fact that voice and full-face photos and comparable images are considered personal health identifiers. As such, like other research data, the informed consent should include information on:

- How the video, audio, or photographs will be obtained, e.g., record/video a focus group or interview session, ask participants to take images or recordings of some aspect of their lives, use images from medical records (HIPAA)
- What will be recorded or photographed (voice only, video or photo to include facial features, photo of a discreet portion of the body to document a medical condition)
- How the video/audio/photograph will be used (e.g., educational purposes), create more accurate record of research proceedings, for commercial use)
- If audio or video recordings will be transcribed, who will transcribe the recordings, and will the transcription be stripped of any personal identifying information or will it be coded to protect each participant's identity
- Where the audio, video, or images will be, stored (secured location such as behind a firewall)
- Who will have access to the audio, video, or images (study staff, contracted individuals for transcription)
- How the audio, video, or images will be protected (e.g. password-protected access)
- How long the images and/or recordings will be retained, and when and how they will be destroyed, if at all

It is recommended that the consent form include a separate heading to specifically address the issues inherent in the collection of research data using video/audio/photography recordings. Investigators may consider informed consent form language that gives participants the opportunity to state the level to which they agree to have their video/audio/photograph recording data used for various purposes. Additionally, if the recording is not required as part of the research study, it must be clearly stated in the consent form along with a way for a participant to select whether or not to be recorded.

Finally, investigators should only record what is necessary for the study and take all steps necessary to blur or obscure the images of those who have not consented to the research and/or to be recorded/photographed.

Below are model statements investigators may adapt to describe recording tools.

Sample: Video and Audio Recordings

[In this section, explain in detail the specific procedures that will be used to protect the study records and subjects' identity. Include a statement describing how electronic files and data will be secured, maintained, and disposed of. Include the following suggested statements for studies involving video and

This material is the work of the Regulatory Foundations, Ethics, and Law Program, part of the Harvard Catalyst | The Harvard Clinical and Translational Science Center. Funded by NCATS (UL1TR002541).

audio recordings, participants must have the option of whether or not to consent to each use of their recordings]. Please indicate whether you consent to each of the following:

_____I agree that segments of the recordings made of my participation in this research may be used for conference presentations, as well as education and training of future investigators/practitioners.

_____I agree to have my recordings archived for future research in the field of [insert area/field of research for which the recordings will be use]).[25]

Sample: Video Recording of Study Activities
Interviews may be recorded using video devices. Recordings will assist with accurately documenting your responses. You have the right to refuse the video recording. Please select one of the following options: I consent to video recording: Yes _____ No _____

Sample: Audio Recording of Study Activities
Interviews may be recorded using audio recording devices. Recordings will assist with accurately documenting your responses. You have the right to refuse the audio recording. Please select one of the following options: I consent to audio recording: Yes _____ No _____

Sample: Photographing of Study Activities/Participants
Photographs of participants may be taken to preserve an image related to the research. You have the right to refuse to allow photographs to be taken. Please select one of the following options: I consent to photographs: Yes _____ No _____ [26]

Sample: Interview Recording
Please sign below if you are willing to have this interview recorded [specify audio or video]. You may still participate in this study if you are not willing to have the interview recorded.[27]

Sample: Focus Group Recording
The use of video/audio recording for this study has been chosen over taking handwritten notes because [insert reason]. You have the right to withdraw from this study if you choose to not be video/audio recorded. Please be advised that although the investigators will take every precaution to maintain confidentiality of the data, the nature of focus groups prevents the investigators from guaranteeing confidentiality. The investigators would like to remind participants to respect the privacy of your fellow participants and not repeat what is said in the focus group to others outside of the group.

The video/audio from the focus group may be used for [future research studies, educational purposes, conference presentations, etc.] You have the right to refuse the use of the video/audio recording for future use. Please select one of the following statements: I consent to the future use of my video/audio recording from this focus group: Yes ____ No____

Sample: Use of Recording
The recording(s) will be used for [include purpose of recording; e.g., sample language may include:

[25] "Informed Consent Template -Video Use." *UMassAmherst*. Web. 6 Jan. 2016. <http://www.umass.edu/research/form/informed-consent-template-video-use>.
[26] "Informed Consent Requirements." *University of Tennessee*. Web. 6 Jan. 2016. <https://www.utc.edu/research-integrity/institutional-review-board/informedconsent/#AV>.
[27] "Informed Consent Form." *University at Albany*. Web. 6 Jan. 2016. <http://www.albany.edu/orrc/irb-forms.php>.

analysis by the research team; possible use as a teaching tool to those who are not members of the research staff (i.e. for educational purposes); commercial purposes. If the tapes will be used for commercial purposes, the consent must specifically state whether the subject would be compensated for this use.]

The recording(s) will include [indicate whether the subject's name or any other identifier will be recorded. If videotaping will be utilized, indicate the extent to which subject's identity would be masked (e.g., facial features partially blocked; recording will not include facial pictures; recording will include full facial pictures.]

The recording(s) will be stored [include measures taken to protect subjects privacy. For example: in a locked file cabinet with no link to subjects' identity; in a locked file cabinet and linked with a code to subjects' identity; in a locked file cabinet and labeled with subjects' name or other identifiable information] and will be [indicate the length of time the recording(s) will be retained, e.g. destroyed upon completion of the study procedures; destroyed upon publication of study results; retained indefinitely.] [28]

Sample: Use of Recording for Educational Purposes

We may wish to present some of the tapes from this study at scientific conventions or as demonstrations in classrooms. Please sign below if you are willing to allow us to do so with your recording.

I hereby give permission for the video/audio tape made for this research study to be also used for educational purposes and to maintain the confidentiality of the information on that tape.[29]

[28] *Columbia University*. Web. 6 Jan. 2016. <http://www.columbia.edu/cu/irb/policies/documents/Informed_Consent_Policysurrogateconsent040110FinalDraft.pdf>.
29 "Technology Services." Moody College of Communication. University of Texas at Austin. Web. 13 Apr. 2016. <http://moody.utexas.edu/technology/video-audio>.

Glossary of Terms

Application (App): App is an abbreviated form of the word "application." 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.[30] *For Health-related mobile apps, please see the definition below.*

Archived Computer Data: A collection of computer files that have been collected for backup purposes. Computer data may be archived for storage, future use, and/or to move the data to another location. The data that is archived can be a list of file names and folders, or the files can be organized in a directory to help with ease of future use.[31]

Blog: A website used as a journal; can be personal or professional in nature.[32]

Chat room: An online location where individuals can come together to have text-based chat discussions that occur in real time.[33]

Cloud computing: Delivery of services, such as storage and applications, over the Internet.[34]

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 without permission to others in ways that are inconsistent with the understanding of the original disclosure.[35]

Cookie: 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.[36]

Covered Entity: An organization or corporation that directly handles Protected Health Information (PHI) or Personal Health Records (PHR). HIPAA defines covered entity as "health plans, health care clearing houses, and health care providers who electronically transmit health information." [1] HIPAA-covered entities must comply with the HIPAA Rules to protect the privacy and security of health information and must providing individuals with certain respect to their health information. [37]

Data Grab: A low-cost and anonymous system that allows for the capture of customer behavior data.[38]

End User Licensing Agreement (EULA): A legal contract between a software developer or vendor and the user of the software. It specifies in detail the rights and restrictions that apply to the software. Although there are big differences among EULAs, typical components are definitions, a grant of license,

---

[30] Rouse, Margaret. "What Is App? - Definition from WhatIs.com." SearchMobileComputing. Nov. 2011. Web. 08 Apr. 2016. <http://searchmobilecomputing.techtarget.com/definition/app>.
[31] Rouse, Margaret. "What Is Data Archiving? - Definition from WhatIs.com." *SearchDataBackup*. Sept. 2015. Web. 06 Apr. 2016. <http://searchdatabackup.techtarget.com/definition/data-archiving>.
[32] Byrd, Kenneth. "What Is a Blog? - Blog Basics." *Blog Basics*. 2011. Web. 06 Apr. 2016. <http://blogbasics.com/what-is-a-blog/>.
[33] *Internet-Based Research-CPHS University of California, Berkley Cphs.berkeley.edu/internet_research.pdf*. Berkeley, CA: University of California, Berkeley, 07 July 2015. PDF.
[34] 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>.
[35] "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>.
[36] *Internet-Based Research-CPHS University of California, Berkley Cphs.berkeley.edu/internet_research.pdf*. Berkeley, CA: University of California, Berkeley, 07 July 2015. PDF.
[37] "Covered Entities and Business Associates." *HHS.gov*. Office for Civil Rights, 2015. Web. 06 Apr. 2016. <http://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html>.
[38] "Data Grab Data In Motion Customer Intent Notification System."*Hackathon.io*. Web. 06 Apr. 2016. <http://www.hackathon.io/30025>.

limitations on use, a copyright notice and a limited warranty. Some EULAs also provide detailed lists of what may and may not be done with the software and its components.[39]

Handheld device: A portable computing or electronic device, typically small enough to fit in the hand.[40]

Health-related mobile app: A mobile application designed to capture health-related information. The most common uses for a health-related mobile app are fitness and nutrition tracking. Often referred to as a "health app." [41]

HIPAA: Health Insurance Portability and Accountability Act of 1996 is United States legislation that provides privacy standards to protect patients' medical records and other health information provided to health plans, doctors, hospitals, and other healthcare providers. [42]

Interactive Multimedia: A computer-delivered electronic system that allows the user to control, combine, and manipulate different types of media, such as text, sound, video, computer graphics, and animation. Interactive multimedia integrates computer, memory storage, digital (binary) data, telephone, television, and other information technologies.[43]

Internet Service Provider (ISP): A company that provides you with access to the Internet (usually with a fee) through various technologies such as: dial-up, cable, Digital Subscriber Line (DSL), Integrated Services Digital Network (ISDN), etc.[44]

Internet: Global network of computers that connects to other devices to send and receive information by dedicated routers and servers.[45]

Mobile: Refers to the ability to provide untethered functionality.[46]

Mobile Device: Anything that can be used on the move and unwired, ranging from Wi-Fi-enabled laptops and mobile phones, to wireless devices that can communicate via Federal Communications Commission (FCC)-allocated frequency. A mobile device is a computing device that can easily be carried or moved, such as a smartphone, tablet computer, portable hard drive (e.g., flash drives, USB memory sticks, or similar storage devices).[47]

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

[39] "EULA Definition." *EULA Definition by The Linux Information Project*. Linux Information Project, 02 Apr. 2004. Web. 06 Apr. 2016. <http://www.linfo.org/eula.html>.
[40] "What Is a Handheld? - Definition from Techopedia." *Techopedia.com*. Web. 06 Apr. 2016. <https://www.techopedia.com/definition/16322/handheld>.
[41] "U.S. Food and Drug Administration." *Mobile Medical Applications*. Web. 08 Apr. 2016. <http://www.fda.gov/MedicalDevices/DigitalHealth/MobileMedicalApplications/default.htm>.
[42] http://www.medicinenet.com/script/main/art.asp?articlekey=31785
[43] The Editors of Encyclopaedia Britannica. "Interactive Multimedia."*Encyclopaedia Britannica Online*. Encyclopaedia Britannica. Web. 08 Apr. 2016. <http://www.britannica.com/technology/interactive-multimedia>.
[44] "What Is an Internet Service Provider?" *WhatIsMyIPAddress.com*. Web. 06 Apr. 2016. <http://whatismyipaddress.com/isp>.
[45] Tyson, Jeff. "Howstuffworks "How Internet Infrastructure Works""*Howstuffworks "How Internet Infrastructure Works"* Web. 06 Apr. 2016. <http://web.stanford.edu/class/msande91si/www-spr04/readings/week1/Howstuffworks.htm>.
[46] Brandt, Jeffrey L., and Stacie Durkin. "Mobile Medical App & Medical Device Regulations." *A Snapshot of MHealth Privacy and Security*. Healthcare Information and Management Systems. Web. 06 Apr. 2016.
[47] Brandt, Jeffrey L., and Stacie Durkin. "A Snapshot of MHealth Privacy and Security." *A Snapshot of MHealth Privacy and Security*. Healthcare Information and Management Systems. Web. 06 Apr. 2016. <http://www.himss.org/ResourceLibrary/mHimssRoadmapContent.aspx?ItemNumber=30548>.

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. [48]

Multimedia: The use of computers to present a combination of interactive content from different content forms such as: text, graphics, audio, video.[49]

Privacy: The right to keep personal information private, as opposed to the general public[50].

Protected Health Information (PHI): Individually identifiable health information that is transmitted or maintained in electronic media or other form or medium that is created or collected by a "covered entity," and can be linked to an individual.[51]

Secure File Transfer Protocol (SFTP): A network that enables file access, transfer, and management over a secured file transferring system.[52]

Secure Socket Layer (SSL): A technology that manages server and client authentication to establish encrypted transmission of communications over the Internet.[53]

Server: A computer program that provides services to other computer programs (and their users) in the same or other computers. Servers are used to manage the resources of a collection of computers or other devices.[54]

Smart Technology: An electronic device or system that can be connected to the Internet, used interactively, and can have some intelligence to monitor and analyze activity.[55]

Third-Party Services: 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. [56]*For more information on third-party services, please see the Federal Trade Commission website.*

Tracking Cookies: Small pieces of data sent from a website and stored in the user's web browser that help a third party identify the user or computer. Cookies are not viruses but can track your online use and share personal information for the server to use to customize web pages.[57]

Web Application: A program that is stored on a remote server and delivered over the Internet on a browser.[58]

---

[48] 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>.
[49] "More about Multimedia." *Dice.com*. Web. 06 Apr. 2016. <https://www.dice.com/skills/Interactive Multimedia.html>.
[50] "private." West's Encyclopedia of American Law, edition 2. 2008. The Gale Group 14 Jun. 2016 http://legal-dictionary.thefreedictionary.com/private.
[51] "HIPAA Privacy Rule and Its Impacts on Research." *HIPAA Privacy Rule and Its Impacts on Research*. 02 Feb. 2007. Web. 06 Apr. 2016. <https://privacyruleandresearch.nih.gov/pr_07.asp>.
[52] "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>.
[53] Rouse, Margaret. "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>.
[54] Rouse, Maragret. "What Is Server? - Definition from WhatIs.com."*WhatIs.com*. TechTarget, June 2014. Web. 06 Apr. 2016. <http://whatis.techtarget.com/definition/server>.
[55] Van Doorn, Menno. "What Does SMART Technology Actually Mean?"*SogetiLabs*. 26 Mar. 2014. Web. 06 Apr. 2016. <http://labs.sogeti.com/wat-smart-technology-actually-mean/>.
[56] "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>.
[57] "Online Privacy: Using the Internet Safely." *Privacy Rights*. Privacy Rights Clearinghouse, Jan. 2016. Web. 06 Apr. 2016. <https://www.privacyrights.org/online-privacy-using-internet-safely>.
[58] Rouse, Maragret. "What Is Web Application (Web App)? - Definition from WhatIs.com." *SearchSoftwareQuality*. TechTarget, July 2011. Web. 06 Apr. 2016. <http://searchsoftwarequality.techtarget.com/definition/Web-application-Web-app>.

This material is the work of the Regulatory Foundations, Ethics, and Law Program, part of the Harvard Catalyst | The Harvard Clinical and Translational Science Center. Funded by NCATS (UL1TR002541).

Web Beacon: 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.[59]

Web Service: Client and server applications that allow for communication between two electronic devices over a network.[60]

Wireless: Telecommunications in which electromagnetic waves (rather than some form of wire) carry the signal over part or all of the communication path. Some monitoring devices, such as intrusion alarms, employ acoustic waves at frequencies above the range of human hearing; these are also sometimes classified as wireless.[61]

Wireless Device: Includes anything that uses a wireless network to either send or receive data. [62]

[59] Beal, Vangie. "Web Beacon." *What Is Web Beacon? Webopedia Definition*. Webopedia. Web. 06 Apr. 2016. <http://www.webopedia.com/TERM/W/Web_beacon.html>.
[60] "Web Services Solution | Cousins Infotech." *Cousins Infotech*. Web. 06 Apr. 2016. <http://www.cousinsinfotech.com/web-services/>.
[61] Rouse, Maragret. "What Is Wireless? - Definition from WhatIs.com."*SearchMobileComputing*. TechTarget, Apr. 2006. Web. 06 Apr. 2016. <http://searchmobilecomputing.techtarget.com/definition/wireless>.
[62] Brandt, Jeffrey L., and Stacie Durkin. "A Snapshot of MHealth Privacy and Security." *A Snapshot of MHealth Privacy and Security*. Healthcare Information and Management Systems. Web. 06 Apr. 2016.

Resources

Clinical Leader: Orri, Miguel. "Electronic Informed Consent: Considerations For Implementation In Clinical Trials." 23 Feb. 2015. *http://www.clinicalleader.com/doc/electronic-informed-consent-considerations-for-implementation-in-clinical-trials-0001*.

Columbia University Human Research Protection Program: "Columbia University Institutional Review Board Policy: Informed Consent" *http://www.columbia.edu/cu/irb/policies/documents/Informed_Consent_Policysurrogateconsent040110FinalDraft.pdf*.

Curtin University (Australia): National Drug Research Institute: "Encryption Guide" for the *Drugs on Forums* project. *http://ndri.curtin.edu.au/drugsonforums/encryption.cfm*.

Facebook, Inc.: "Facebook Privacy." https://www.facebook.com/about/privacy/.

Harvard Catalyst:

- "Guidance for Researchers Using Internet Cloud Computing Services and Apps." *https://catalyst.harvard.edu/pdf/regulatory/CloudGuidanceResearchers.pdf*.
- "Guide to Technologies Used in Research." *http://catalyst.harvard.edu/pdf/regulatory/Investigators%20Guide%20to%20RDM%20practice.pdf*.

Inter-University Consortium for Political and Social Research at University of Michigan: "Recommended Informed Consent Language for Data Sharing." *http://www.icpsr.umich.edu/icpsrweb/content/datamanagement/confidentiality/conf-language.html*.

Lawrence Technological University: "Office of the Provost: Institutional Review Board." *http://www.ltu.edu/provosts_office/irb.asp*.

MailChimp: "Terms of Use | MailChimp." *http://mailchimp.com/legal/terms/?_ga=1.62751336.532882110.1449240608*.

Multi-Regional Clinical Trials (MRCT): "The MRCT Center of Brigham and Women's Hospital and Harvard." *http://mrctcenter.org/*.

The Petrie-Flom Center for Health Law Policy, Biotechnology, and Bioethics at Harvard Law School: "The Use of Social Media in Recruitment to Clinical Trials: A Guide for Investigators and IRBs." *http://petrieflom.law.harvard.edu/assets/publications/PFCannualreport12_13.pdf*.

Privacy Laws & Business (UK): "No Need for Informed Consent for Authentication and Session-ID Cookies - Privacy Laws & Business." 12 Jun. 2012.

This material is the work of the Regulatory Foundations, Ethics, and Law Program, part of the Harvard Catalyst | The Harvard Clinical and Translational Science Center. Funded by NCATS (UL1TR002541).

https://www.privacylaws.com/Publications/enews/International-E-news/Dates/2012/6/No-need-of-informed-consent-for-authentication-and-session-ID-cookies/.

Rutgers University: "Consent Form to Take Part in a Mobile/Electronic Device or Technology Study." *http://comminfo.rutgers.edu/~cgal/IRB.pdf*.

Sunnybrook Research Institute: "Secondary Use of Data - FAQs - Research Ethics Office." *http://sunnybrook.ca/research/content/?page=sri-crs-reo-faq-secondaryusedata*.

TechTarget: Sheldon, Robert. "Wireless Carrier Security Risks: Keeping Enterprise Data Safe." Apr. 2012. *http://searchmobilecomputing.techtarget.com/tip/Wireless-carrier-security-risks-Keeping-enterprise-data-safe*.

TED Talks:

- "Why Privacy Matters." *http://www.ted.com/talks/glenn_greenwald_why_privacy_matters*.
- "Tracking Our Online Trackers." *http://www.ted.com/talks/gary_kovacs_tracking_the_trackers*.

Twitter, Inc.: "Twitter Privacy Policy." *https://twitter.com/privacy?lang=en*.

University of Albany Division for Research:

- "Institutional Review Board Electronic Data Management Policy." *http://www.albany.edu/orrc/assets/Institutional_Review_Board_Data_Management_Policy_v_1_0.pdf*.
- "Informed Consent Form." *http://www.albany.edu/orrc/irb-forms.php*.

University of California, Berkeley Research Administration and Compliance: "Internet Based Research." *http://cphs.berkeley.edu/internet_research.pdf*.

University of California, San Francisco Office of Ethics and Compliance: "Human Research Protection Program." *http://irb.ucsf.edu/*.

University of Massachusetts, Amherst Research Administration & Compliance:
"Forms & Templates." *https://www.umass.edu/research/compliance/human-subjects-irb/forms*.
"Informed Consent Template -Video Use." *http://www.umass.edu/research/form/informed-consent-template-video-use*.

University of Montana: "Informed Consent Form Template." *https://www.umt.edu/research/compliance/IRB/Docs/consent.doc*.

University of Notre Dame: "Special Considerations in IRB Review." *http://or.nd.edu/research-compliance/human-subjects-research/irb-procedures-manual-guidelines/special-considerations-in-irb-review/*.

This material is the work of the Regulatory Foundations, Ethics, and Law Program, part of the Harvard Catalyst | The Harvard Clinical and Translational Science Center. Funded by NCATS (UL1TR002541).

University of Pittsburgh Human Research Protection Office:
"Consent Form-Suggested Wording." *http://www.irb.pitt.edu/consent-form-suggested-wording.*
"Electronic Data Security." *http://www.irb.pitt.edu/electronic-data-security*.

University of Tennessee: "Informed Consent Requirements." *http://www.utc.edu/research-integrity/pdfs/irb-avlanguageexample.pdf*.

University of Texas at Austin: "Technology Services." Moody College of Communication. *http://moody.utexas.edu/technology/video-audio*.

U.S. Department of Health and Human Services:
"Internet Research and Human Subjects Research Regulations." *http://www.hhs.gov/ohrp/sachrp-committee/recommendations/2013-may-20-letter-attachment-b/#*.

U.S. Department of Veterans Affairs: "VA Informed Consent Form." *http://www.va.gov/*.

U.S. Food and Drug Administration: "Use of Electronic Informed Consent in Clinical Investigations." *http://www.fda.gov/downloads/Drugs/GuidanceComplianceRegulatoryInformation/Guidances/UCM436811.pdf*.

Vanderbilt University: "Efforts to Protect Confidentiality." *http://www.vanderbilt.edu/litspace/Synchrony/confidentialBottom.html#confidentiality*.

Washington University in St. Louis: REDCap: "Boilerplate Language for Inclusion in Grants and IRB Documentation." *http://www.biostat.wustl.edu/redcap/?page_id=242*.

WhatAreCookies.com: "Cookies." *http://www.whatarecookies.com/*.

This material is the work of the Regulatory Foundations, Ethics, and Law Program, part of the Harvard Catalyst | The Harvard Clinical and Translational Science Center. Funded by NCATS (UL1TR002541).

Terms of Use

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 sample informed consent language

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 named authors.

- **Suggested citation:** *This material is the work of the Harvard Catalyst Emerging Technologies Ethics, and Research Data Committee 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 UL1TR002541 and financial contributions from Harvard University and its affiliated academic health care 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 regarding who is using the materials and how they are using it. We may contact you by email to solicit information on how you have used the materials, 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 to include a link to the web page containing this guide.
- **When adapting:** Please share with us improvements to the tool so we may learn and improve our materials as well.

This material is the work of the Regulatory Foundations, Ethics, and Law Program, part of the Harvard Catalyst | The Harvard Clinical and Translational Science Center. Funded by NCATS (UL1TR002541).

Acknowledgments

We thank the Harvard Catalyst Emerging Technologies, Ethics, and Research Data committee (formerly the IRB-IT Task Force) of the Regulatory Foundations, Ethics, and Law Program whose work made this tool possible.

Core Writing Group

Sabune Winkler	**Harvard Catalyst**
Joanna Myerson	Harvard Catalyst
Steve Berry	Beth Israel Deaconess Medical Center
Jessica Biggers	Harvard Catalyst
Kris Bolt	Multi-Regional Clinical Trials Center
Betsy Draper	Harvard Faculty of Arts and Sciences
Scott Edmiston	Harvard Medical School
Lisa Gabel	Harvard Longwood Medical Area
Sara Harnish	Dana Farber Cancer Institute
Fariba Houman	Mass. Eye and Ear
P. Pearl O'Rourke	Partners Healthcare
Ian Poynter	Broad Institute
Pamela Richmond	Hebrew Senior Life
Jason Rightmyer	Hebrew Senior Life
Paul Scheib	Boston Children's Hospital
Sandra Silk	Harvard University
Lynn Simpson	Partners Healthcare
Paula Tebeau	Harvard Pilgrim Healthcare
Mark Tomilson	Dana Farber Cancer Institute
Joe Zurba	Harvard Medical School
Barbara E. Bierer	Harvard Catalyst and Brigham and Women's Hospital

Contributors

Recognizing those that contributed specific content, editing, or examples included in this document:

Elizabeth Witte, Editor	Harvard Catalyst
Luke Gelinas	Petrie-Flom Center/Harvard Catalyst Fellow in Clinical Research Ethics

Contact Us

Please send any suggestions, feedback, or questions regarding this consent library to regulatory@catalyst.harvard.edu.

This material is the work of the Regulatory Foundations, Ethics, and Law Program, part of the Harvard Catalyst | The Harvard Clinical and Translational Science Center. Funded by NCATS (UL1TR002541).