Privacy Safeguards

At Stanford University, we have an obligation to respect and safeguard the information of our patients and research participants. The School of Medicine Privacy Office has created this safeguards document that describes the practical steps that we all can take on a daily basis to protect the information that we maintain.

Throughout this document there are references to Protected Health Information (PHI) and "other sensitive data." As a reminder, PHI includes:

- Name, address, date of birth, age, contact information
- Medical records, x-rays, lab results, photographs, prescriptions
- Billing statements, insurance information, social security numbers
- Research data

For the purposes of this document, "other sensitive data" encompasses the data that falls under the confidential, restricted and prohibited categories in Stanford University's Data Classification Guidelines.

Information must be protected whether it's in written, verbal or electronic form.

Information Security

Visit the School of Medicine's Data Security Website. For the most up-to-the-minute information on the School of Medicine's Data Security Program, visit http://med.stanford.edu/datasecurity.

Back-up and encrypt devices. The School of Medicine Data Security Policy mandates centrally-managed data backup and encryption services for all computers and mobile devices used for Stanford business, including personally-owned devices. This applies to all members of the SoM community, including faculty, staff, students, residents, post-docs, fellows and other Stanford affiliates. This includes desktop computers, laptops, iPhones, iPads, other smartphones and tablets, USB flash drives, etc. Even if your device is only used to access your @stanford.edu email, it must be backed-up and encrypted. Contact the School of Medicine IRT Service Desk at X5-8000 if you have questions.

Personal mobile devices. If you use your personal mobile device for work purposes (including to access your @stanford.edu email), you are required to encrypt your device. If you are using an iPhone or iPad see the Stanford MDM section below. If you are using a mobile device other than an iPhone or iPad, contact your local IT department for assistance with securing your device.

Enroll in Stanford's MDM service. Stanford's Mobile Device Management (MDM) service is a free, self-install service that safeguards your Apple iOS device (iPhone, iPad, iPod Touch) by ensuring certain information security protections are activated. This includes a longer password, encryption and a remote wipe capability. Visit http://mdm.stanford.edu from the web browser of your Apple iOS device to complete this quick, self-install. Contact the School of Medicine IRT Service Desk at X5-8000 if you have questions.

Use of personal email accounts. You should not use a personal email account to conduct Stanford-related business. In addition, your @stanford.edu email account should **not** be configured to forward your Stanford email to a personal email account, such as Gmail, if there is any possibility that you might send or receive PHI or other sensitive data.

Information Security (cont.)

Data Management. Whenever possible, avoid using Excel to save large amounts of PHI or other sensitive information, or to create document/databases that will be shared and updated often. Excel does not offer such key safeguards as version control, user logging and user control. As an alterative, use Stanford's REDCap application (Research Electronic Data Capture). REDCap is an excellent alternative to Excel or simple Filemaker/Access databases as it is approved by Stanford, web-accessible, secure, and is free of charge. To learn more about how REDCap may fit your needs, visit http://redcap.stanford.edu.

Report lost or stolen devices immediately. Notify the School of Medicine Privacy Office **immediately** at medprivacy@stanford.edu or 650.725.1828 if a device has been lost or stolen. Federal and state privacy laws require Stanford to take very specific actions within very limited timelines, based on the circumstances of the incident.

Email

Verify the recipient's email address. Many email programs will auto-populate email addresses as you begin to type characters in the to:, cc:, and bcc: fields. Always ensure, that you have typed or selected the recipient's correct email address.

Email the minimum necessary. Emailing the minimum necessary PHI helps to ensure that the recipient only receives the information that they have a legitimate business need to receive.

Send emails from a Stanford email address. Emails pertaining to Stanford business and recruitment should always be sent from your Stanford email address (@stanford.edu, @stanfordmed.org, or @lpch.org). This establishes credibility and ensures that the appropriate information security safeguards are in place.

Avoid group emails. If you need to send the same email to multiple recipients either send the emails individually, or use the bcc: field. Do **not** use the to: or cc: fields when sending an email to multiple recipients.

Use a Stanford-approved Secure Email system to email PHI. Stanford's Secure Email service is approved for emailing PHI. All you need to do is to insert "secure:" in the subject line of any message you are sending. Doing so will ensure the security of the contents of the message, whether it is sent to someone at Stanford or outside of Stanford. To learn more about Stanford's Secure Email service, visit http://secureemail.stanford.edu. If you have a need to securely send large files, use Stanford's Med Secure Send service. To learn more, visit http://med.stanford.edu/irt/security/mss.html.

Consider alternatives to sending PHI via email. In order to view an email sent from Stanford's Secure Email service, the recipient will have to first register for an account within the Secure Email service, or sign in with an existing account (instructions for both are automatically provided to the recipient). If the recipient has difficultly registering for or navigating Stanford's Secure Email system, either take the conversation offline (e.g. telephone) or avoid sending PHI in the email.

Take emails containing PHI offline. If someone sends you an email that contains PHI, consider responding with a phone call rather than replying to the email – this ensures that PHI does not continue to be emailed. Let the person know that you would like to take the dialog offline so as to ensure their privacy. If you cannot take the dialog offline, and need to reply to an email that contains PHI (even if someone else sent it to you), you will either need to send it using Stanford's Secure Email system, **or,** remove all PHI from the entire email string prior to sending.

Paper

Utilize off-site storage. Paper records that do not need to be kept on-site – but cannot yet be destroyed – should be sent to off-site storage. This is an especially important safeguard in "open plan" office environments where secure storage spaces (e.g. lockable filing cabinets) are in limited supply.

Store PHI electronically. Whenever possible, paper files that need to be maintained in the office should be converted to electronic versions that are stored on devices that are both access-controlled and encrypted. Again, in "open plan" office environments this is an especially important consideration.

Securely destroy PHI. Paper files that are no longer needed should be securely disposed of in secure shredding bins which are located in most buildings. Contact the School of Medicine Information Security office at irt-security@lists.stanford.edu for information on how to securely destroy devices containing PHI (e.g. hard drives, CD's etc.).

Keep PHI secure. Whenever possible, PHI should be secured in locked drawers or cabinets, even when in an access-controlled building. This applies to PHI in paper and electronic form (e.g. research study-related binders and files, cameras, external hard drives, flash drives, smartphones, etc.) This helps to ensure that only those who truly have a business need to access the information will have access to it.

Label generically. Binders, boxes, storage devices, files or folders that contain PHI should be labeled as generically as possible, without displaying PHI or any individually identifiable information.

Research Participant Recruitment

"New Media" Recruitment. Online media platforms provide excellent opportunities for research study recruitment. Whether you wish to recruit research participants via social media such Facebook, Twitter, Google+ or via online ads such as Google AdWords and Microsoft adCenter, these "new media" recruitment methods should be treated like traditional advertising methods, i.e., follow IRB's guidelines for traditional ads. Remember, the Stanford contact information should always be a Stanford email address (@stanford.edu, @lpch.org, or @stanfordmed.org).

Secure Surveys. Avoid using traditional online survey systems like "Survey Monkey" to collect information from research participants. If you have a need to collect information from research participants via an online survey, use one of Stanford's approved and secure applications: **Qualtrics** (http://stanfordmedicine.qualtrics.com) or **REDCap Survey** (http://redcap.stanford.edu). Both Qualtrics and REDCap Survey are approved for collecting and storing PHI and include such key features as branching logic, multiple pages, email to participants, etc.

Privacy Incident Reporting

Report immediately. If you suspect that a privacy incident has occurred, the most important thing you can do is to contact the School of Medicine Privacy Office **immediately** at medprivacy@stanford.edu or 650.725.1828. Federal and state privacy laws require Stanford to take very specific actions within very limited timelines, based on the circumstances of the incident.