Basic Privacy and Security Principles

Stanford HEALTH CARE

Protecting Patient Privacy

. . . one patient at a time

Basic Privacy and Security Principles

Stanford HEALTH CARE

Welcome to the "Protecting Patient Privacy" course.

Instructions: Before you begin this course, please note the following:

- For the purposes of this course, the term **"Stanford"** is used collectively to represent Stanford Children's Health (SCH), Stanford Hospital & Clinics (SHC), Stanford University School of Medicine and certain departments within Stanford University.
- For the purposes of this course, the term **"Patient"** is used collectively to include patients at Stanford Children's Health and Stanford Hospital & Clinics, ***as well as School of Medicine research participants.***
- For purposes of this course, the term "**Patient Information"** is used collectively to include information about patients at Stanford Children's Health and Stanford Hospital & Clinics, ***as well as information about School of Medicine research participants.***
- ***If you are involved in the management or design of School of Medicine research studies, (for example, Principal Investigator, Study Designer, Research Coordinator, or Research Associate), you must complete an additional e-Learning module*** through the School of Medicine that focuses on privacy and security standards for the conduct of research.

Basic Privacy and Security Principles

Stanford HEALTH CARE

Instructions: Before you begin this course, please note the following:

- For the purposes of this course, the term **"Supervisor"** or **"Manager"** is sometimes used in the context of approval for certain privacy and security practices, such as supervisor approval for you to conduct work offsite that involves patient information or manager approval for you to use your mobile device to send or receive patient information. ***For senior operational leadership (Directors and above), faculty and physicians on medical staff only***, it is understood that from time-to-time your duties will require you to conduct activities for which this training requires supervisor or management approval. ***Such approval for senior operational leadership, faculty and physicians on medical staff is self-granted provided that all safeguards and other privacy and security controls outlined in this training are in place***. Faculty and physicians should seek direction from the chief medical officer or the chief of staff if unsure about self-approval for any activity involving patient information. The Hospital and University Privacy Offices are available to advise on activities in this training that require supervisor or manager approval.

Basic Privacy and Security Principles

Stanford HEALTH CARE

Section 1

Protecting Patient Privacy. . . One Patient at a Time

1.1 Our Commitment to Protect Patient Privacy

1.2 Information Protected Under the Law

1.3 Preventing Privacy Breaches

1.4 Duty to Immediately Report

1.5 Consequences for Failing to Protect Patient Privacy

Basic Privacy and Security Principles

Stanford HEALTH CARE

Section 1.1: Our Commitment to Protect Patient Privacy

Patients and their families trust us with highly personal and sensitive information regarding their medical conditions. If patients and families do not feel confident that we will keep such information private, they may hesitate to discuss some health concerns with us, which can affect our medical decision making and hinder their medical care.

Stanford is committed to compliance with all applicable patient privacy laws, rules, and regulations and has policies and procedures in place for the protection of patient information. This commitment extends to each of us, regardless of our role in, or relationship with, the organization. As part of this commitment, you are required to protect the privacy and confidentiality of our patients and families and to take conscious steps during your daily activities to prevent the unauthorized or impermissible access to patient information, internal use of patient information, or disclosure of patient information outside the organization. Even when you are no longer working here, you are still bound to maintain the confidentiality of information viewed, received or used during the course of your relationship with the organization.

Basic Privacy and Security Principles

Stanford HEALTH CARE

Section 1.1: Our Commitment to Protect Patient Privacy

Information about patients related to their medical history, their past, present, or future mental or physical condition, their diagnosis or treatment, or their payment for services is protected under California and federal patient privacy laws. These protections apply to all forms of patient information, including patient information that is spoken, written, or in our electronic systems. Laws such as the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health Act (HITECH), and the Confidentiality of Medical Information Act (CMIA) include strict requirements for the protection of patient information. These patient privacy laws apply to the organization, as well as to you as an individual.

Privacy breaches can have a severe impact on the reputation of Stanford. Wherever you work - Lucile Packard Children's Hospital, Stanford Hospital & Clinics, School of Medicine or the University - it is important to take patient and research participant privacy seriously and abide by all privacy and information security policies for your organization.

Basic Privacy and Security Principles

Stanford HEALTH CARE

Section 1.2: Information Protected Under the Law

Information that is protected under the law is often referred to as Protected Health Information (PHI) and applies to both living and deceased patients. PHI is defined as individually identifiable health Information that relates to a patient's past, present or future physical or mental health or condition, the provision of health care to a patient, or the past, present, or future payment for health care provided to a patient.

At a minimum, the following information about a patient or a patient's relatives, employers or household members is considered PHI:

- Names;
- Social Security numbers;
- Telephone numbers;
- Addresses and all geographic subdivisions smaller than a state;
- All elements of dates (except year), including birth date, admission date, discharge date, date of death; and all ages over 89;
- Fax numbers;
- Electronic mail (e-mail addresses);
- Medical Record numbers;

Basic Privacy and Security Principles

Stanford HEALTH CARE

Section 1.2: Information Protected Under the Law

- Medical Record numbers;
- Health Plan Beneficiary numbers;
- Account numbers;
- Certificate/license numbers;
- Vehicle identifiers and serial numbers, including license plate numbers;
- Device identifiers and serial numbers;
- Web Universal Resource Locators (URLs);
- Internet Protocol (IP) addresses;
- Biometric Identifiers, including finger and voice prints;
- Full face photographic images and any comparable images; and
- Any other unique identifying number, characteristic or code.

It is important to note that the last item on the list, "any other unique identifying number, characteristic or code," is intended to be a broad regulatory catch-all so that information not specifically on the list is considered PHI if there is the potential that the information can be used in a broad sense to identify the patient. Recent regulatory guidance gives the example that the occupation of a patient listed in a medical record as "President of State University" would render that fact alone as PHI. Another example given under this concept is when patient-unique barcodes are

Section 1.2: Information Protected Under the Law

Another example given under this concept is when patient-unique barcodes are embedded into patient records or their medications, that barcode alone is considered PHI. Information is PHI if, when used alone or in combination with other information, it could lead to identification of patients. Any actual knowledge that information could be used alone or in combination with other information would make that information PHI. For example, saying "The person who gave birth to octuplets" would be considered PHI. In addition, genetic information is considered PHI. Genetic information includes not only the results of a genetic test, but also genetic counseling, genetic education, and clinical research that includes genetic services. Any genetic service that is requested or received by a patient or patient's family or in which they participate is considered genetic information.

Any single element on the list, standing alone or in combination with other information, is considered PHI and is protected under the law. For instance, a date of service alone or a zip code alone, without a patient name or any other information, is considered PHI and is subject to privacy protections. The fact that a person is a patient or a research participant at Stanford is considered PHI, as is a patient's location while at the hospital. Information derived from identifiers such as those on the above list are also PHI. For example, patient initials or the last four digits of a

Section 1.2: Information Protected Under the Law

Any single element on the list, standing alone or in combination with other information, is considered PHI and is protected under the law. For instance, a date of service alone or a zip code alone, without a patient name or any other information, is considered PHI and is subject to privacy protections. The fact that a person is a patient or a research participant at Stanford is considered PHI, as is a patient's location while at the hospital. Information derived from identifiers such as those on the above list are also PHI. For example, patient initials or the last four digits of a social security number are considered PHI and are subject to the same privacy protections as full names. A patient's medical record or clinical trial record is PHI, but PHI can also be in emails, in job-related conversations that you have with co-workers, in calls that you take from patients, in notes that you take when talking with patients or physicians, in images and photos, in patient billing statements, in research or publications, in disease-related data bases or registries, in information that is shared with vendors, in faxes that you send or receive, in data reports for quality purposes or financial projections or strategic initiatives, in almost everything we do at the hospital or School of Medicine. You should assume that all information that you access, use or disclose - in any form, verbal, electronic or physical - about patients or their relatives is subject to the law and must be safeguarded.

Basic Privacy and Security Principles

Stanford HEALTH CARE

Section 1.3: Preventing Privacy Breaches

Each of us has a legal and ethical obligation to apply appropriate safeguards for the protection of patient privacy. You have a duty to ensure that your access to, use, and disclosure of patient information is appropriate, and to ask questions if you are unsure about privacy requirements.

According to the U.S. Department of Health and Human Services, most privacy breaches are preventable. The most common causes of major privacy breaches include theft or loss of laptops/cell phones/flash drives/backup tapes, sending unencrypted email, not terminating access to systems when employees are terminated, snooping into patient records, misdirecting mail and faxes, and not shredding paper PHI or otherwise not appropriately destroying PHI. Taking care to apply appropriate safeguards to protect PHI in our daily work routines may prevent most of these privacy breaches from occurring.

State and federal privacy laws require us to notify patients and research participants in the event of certain privacy breaches. Stanford's Privacy Offices will handle all privacy breach notifications. Never communicate independently with a patient about a potential or actual privacy breach. Contact your Privacy Office immediately if you are aware of a potential or possible privacy breach. The Privacy Office will notify

< PREV

Section 1.3: Preventing Privacy Breaches

unencrypted email, not terminating access to systems when employees are terminated, snooping into patient records, misdirecting mail and faxes, and not shredding paper PHI or otherwise not appropriately destroying PHI. Taking care to apply appropriate safeguards to protect PHI in our daily work routines may prevent most of these privacy breaches from occurring.

State and federal privacy laws require us to notify patients and research participants in the event of certain privacy breaches. Stanford's Privacy Offices will handle all privacy breach notifications. Never communicate independently with a patient about a potential or actual privacy breach. Contact your Privacy Office immediately if you are aware of a potential or possible privacy breach. The Privacy Office will notify patients when needed in accordance with state and federal privacy laws.

In the event of a potential or actual privacy breach, you will be expected to fully cooperate with the investigation. In the event that patients need to be notified, care providers with whom the patient has a relationship may be required to participate in the notification process.

Basic Privacy and Security Principles

Stanford HEALTH CARE

Section 1.4: Duty to Immediately Report

You are required to immediately report suspected or actual privacy violations of patient privacy to the SCH/SHC Compliance Department's Privacy Office or to the University's Privacy Office. Delays in reporting or failure to report immediately to the Privacy Office may result in disciplinary action, up to and including termination. The Privacy Office will evaluate all reports promptly, completely and fairly.

You can report privacy concerns to the SCH/SHC Privacy Office in one of the following ways:

- ***Contact the Compliance Department's Privacy Office directly by calling 650-724-2572***
- ***Email your concern to PrivacyOfficer@stanfordmed.org***
- ***Fax your concern to 650-736-8272***
- ***Call the Compliance and Privacy 24 hour Hotline at 800-216-1784, including making anonymous reports***

You can report privacy concerns to the University Privacy Office in one of the following ways:

PREV

Basic Privacy and Security Principles

Stanford HEALTH CARE

Section 1.4: Duty to Immediately Report

You can report privacy concerns to the University Privacy Office in one of the following ways:

- ***Contact the University's Privacy Office directly by calling 650-725-1828***
- ***Email your concern to medprivacy@stanford.edu***

No adverse actions will be taken against someone for making a report in good faith or for cooperating with a privacy investigation with good intentions. Stanford has policies that protect against retaliation or retribution for reporting a privacy concern in good faith or for cooperating with a privacy investigation with good intentions. The non-retaliation policies ensure that no one is penalized for reporting what is honestly believed to be a privacy problem or for honestly participating in a privacy investigation. However, if someone purposely falsifies or misrepresents a report or makes false statements during an investigation, that person will not be protected under the non-retaliation policies. False accusations or statements made in a report or during an investigation, including those made with the intent of harming or retaliating against another person, may result in disciplinary action, up to and including termination.

< PREV

Section 1.4: Duty to Immediately Report

non-retaliation policies ensure that no one is penalized for reporting what is honestly believed to be a privacy problem or for honestly participating in a privacy investigation. However, if someone purposely falsifies or misrepresents a report or makes false statements during an investigation, that person will not be protected under the non-retaliation policies. False accusations or statements made in a report or during an investigation, including those made with the intent of harming or retaliating against another person, may result in disciplinary action, up to and including termination.

The Privacy Office conducts investigations into potential privacy breaches. Immediately reporting privacy concerns or possible privacy issues to the Privacy Office enables the hospital to meet reporting deadlines mandated by federal and California privacy laws. Generally, the deadline for reporting a privacy breach to government authorities is five days, so it is important that you do not wait even a day and that you immediately report a concern, even on nights and weekends, so that the Privacy Offices can begin their investigation into the matter.

Sometimes Stanford is required by law to report certain privacy issues to state or federal agencies. When this is the case, the Privacy Offices will conduct an evaluation

Section 1.4: Duty to Immediately Report

or during an investigation, including those made with the intent of harming or retaliating against another person, may result in disciplinary action, up to and including termination.

The Privacy Office conducts investigations into potential privacy breaches. Immediately reporting privacy concerns or possible privacy issues to the Privacy Office enables the hospital to meet reporting deadlines mandated by federal and California privacy laws. Generally, the deadline for reporting a privacy breach to government authorities is five days, so it is important that you do not wait even a day and that you immediately report a concern, even on nights and weekends, so that the Privacy Offices can begin their investigation into the matter.

Sometimes Stanford is required by law to report certain privacy issues to state or federal agencies. When this is the case, the Privacy Offices will conduct an evaluation of the issue consistent with state and federal reporting requirements and will notify the appropriate state or federal agencies on behalf of Stanford when applicable. Additionally, the Privacy Office will notify patients when needed and will take steps to mitigate any harmful effects caused by a privacy breach.

Section 1.5: Consequences for Failing to Protect Patient Privacy

Patient privacy laws include serious consequences for failing to protect patient privacy, including potential fines for both Stanford and for you as an individual, imprisonment, and loss of your professional license. Patients have the right to assert legal claims against both Stanford and you personally. The State of California and federal authorities aggressively investigate and enforce privacy and security laws against healthcare institutions and individuals when a compromise to patient information occurs, whether due to intentional wrongdoing or simply a mistake. Additionally, violating our privacy policies can lead to disciplinary actions, up to and including termination.

Carelessness, lapse in judgment, or just failing to stop and think about how a certain action you take, or do not take, might compromise patient privacy and could result in a serious situation for you. Even if a situation is caused by a simple mistake or an unintentional or inadvertent act, harm to our patients could result.

Basic Privacy and Security Principles

Stanford HEALTH CARE

Section 1.5: Consequences for Failing to Protect Patient Privacy *(continued)*

The following are examples in the news where healthcare industry staff failed to take appropriate precautionary measures to protect patient information and as a result suffered severe consequences such as disciplinary action, loss of job, and governmental fines. Click the **red** number to advance through the news articles. Click **DONE** to jump to the next slide.

NOTE: You will not be able to advance until you have read all of the examples.

Stanford HEALTH CARE

Section 1.5: Consequences for Failing to Protect Patient Privacy *(continued)*

The following are examples in the news where healthcare industry staff failed to take appropriate precautionary measures to protect patient information and as a result suffered severe consequences such as disciplinary action, loss of job, and governmental fines. Click the **red** number to advance through the news articles. Click **DONE** to jump to the next slide.

NOTE: You will not be able to advance until you have read all of the examples.

1 2 3 4 5 6 7 8 9 10 11 12

Massachusetts General Hospital Fined $1 Million After Employee Leaves Paper Records on Subway

The U.S. Department of Health and Human Services Office for Civil Rights (OCR) fined Mass General $1 million as a result of an employee accidentally leaving PHI for 192 patients on the subway. Additionally, OCR imposed a three-year corrective action plan that includes oversight and intervention by OCR, including the appointment of an internal monitor on Mass General premises to conduct audits and inspections of employee privacy practices with frequent reporting to OCR on the hospital's HIPAA compliance.

The most serious consequence when we fail to protect patient information is the harm and concern that it can cause our patients. Protecting patient privacy is an integral part of patient care.

DONE

Stanford HEALTH CARE

Section 1.5: Consequences for Failing to Protect Patient Privacy *(continued)*

The following are examples in the news where healthcare industry staff failed to take appropriate precautionary measures to protect patient information and as a result suffered severe consequences such as disciplinary action, loss of job, and governmental fines. Click the **red** number to advance through the news articles. Click **DONE** to jump to the next slide.

NOTE: You will not be able to advance until you have read all of the examples.

1 2 3 4 5 6 7 8 9 10 11 12

UCLA Fined $865,000 and Entered into a Three-Year Corrective Action Plan

UCLA employees snooped into the electronic medical records of celebrity patients. OCR fined the hospital $865,000 and imposed a three-year corrective action plan.

The most serious consequence when we fail to protect patient information is the harm and concern that it can cause our patients. Protecting patient privacy is an integral part of patient care.

DONE

Stanford HEALTH CARE

Section 1.5: Consequences for Failing to Protect Patient Privacy *(continued)*

The following are examples in the news where healthcare industry staff failed to take appropriate precautionary measures to protect patient information and as a result suffered severe consequences such as disciplinary action, loss of job, and governmental fines. Click the **red** number to advance through the news articles. Click **DONE** to jump to the next slide.

NOTE: You will not be able to advance until you have read all of the examples.

Physician Terminated, Fined and Found Guilty of Unprofessional Conduct by State Medical Board

A physician in Rhode Island posted information about some of her emergency room encounters on Facebook.

The Rhode Island Board of Medical Licensure found her guilty of unprofessional conduct and issued a reprimand and fine, even though patient names were not posted.

The most serious consequence when we fail to protect patient information is the harm and concern that it can cause our patients. Protecting patient privacy is an integral part of patient care.

DONE

Section 1.5: Consequences for Failing to Protect Patient Privacy *(continued)*

The following are examples in the news where healthcare industry staff failed to take appropriate precautionary measures to protect patient information and as a result suffered severe consequences such as disciplinary action, loss of job, and governmental fines. Click the **red** number to advance through the news articles. Click **DONE** to jump to the next slide.

NOTE: You will not be able to advance until you have read all of the examples.

1 2 3 4 5 6 7 8 9 10 11 12

Employee Gets Sentenced for Looking At Another's Medical Records

A hospital worker was sentenced in criminal court to a 6- to 12-month suspended jail term, two years on probation and a $2,000 fine for unauthorized access to electronic medical records.

The most serious consequence when we fail to protect patient information is the harm and concern that it can cause our patients. Protecting patient privacy is an integral part of patient care.

DONE

Basic Privacy and Security Principles

Stanford HEALTH CARE

Section 1.5: Consequences for Failing to Protect Patient Privacy *(continued)*

The following are examples in the news where healthcare industry staff failed to take appropriate precautionary measures to protect patient information and as a result suffered severe consequences such as disciplinary action, loss of job, and governmental fines. Click the **red** number to advance through the news articles. Click **DONE** to jump to the next slide.

NOTE: You will not be able to advance until you have read all of the examples.

1 2 3 4 5 6 7 8 9 10 11 12

Employee Fired for Accessing Billing and Registration Information

A Penn State hospital employee accessed the former Penn State football coach's billing and registration records. The employee was terminated.

The most serious consequence when we fail to protect patient information is the harm and concern that it can cause our patients. Protecting patient privacy is an integral part of patient care.

DONE

< PREV

Basic Privacy and Security Principles

Stanford HEALTH CARE

Section 1.5: Consequences for Failing to Protect Patient Privacy *(continued)*

The following are examples in the news where healthcare industry staff failed to take appropriate precautionary measures to protect patient information and as a result suffered severe consequences such as disciplinary action, loss of job, and governmental fines. Click the **red** number to advance through the news articles. Click **DONE** to jump to the next slide.

NOTE: You will not be able to advance until you have read all of the examples.

16 Employees Fired For Accessing Patient Records

Employees impermissibly accessed patient records, including physician and co-worker records, at a county hospital in Texas. The employees were fired.

The most serious consequence when we fail to protect patient information is the harm and concern that it can cause our patients. Protecting patient privacy is an integral part of patient care.

DONE

< PREV

Stanford HEALTH CARE

Section 1.5: Consequences for Failing to Protect Patient Privacy *(continued)*

The following are examples in the news where healthcare industry staff failed to take appropriate precautionary measures to protect patient information and as a result suffered severe consequences such as disciplinary action, loss of job, and governmental fines. Click the **red** number to advance through the news articles. Click **DONE** to jump to the next slide.

NOTE: You will not be able to advance until you have read all of the examples.

1 2 3 4 5 6 7 8 9 10 11 12

Cignet Health fined $4.3 Million for HIPAA Breach

Cignet Health denied 41 patients on separate occasions access to their medical records when requested, which is a violation of the HIPAA Privacy Rule. Cignet Health also failed to cooperate with the OCR investigation. The fine for denying the 41 patients access to their medical records was $1.3 million. Cignet Health was fined $3 million for failing to cooperate with OCR's investigation.

The most serious consequence when we fail to protect patient information is the harm and concern that it can cause our patients. Protecting patient privacy is an integral part of patient care.

DONE

Stanford HEALTH CARE

Section 2

Basic Privacy and Security Principles

2.1 Principle 1: Minimum Necessary

2.2 Principle 2: Need to Know

2.3 Principle 3: Authorized Uses and Disclosures

2.4 Principle 4: Verification

2.5 Principle 5: Safeguards

2.6 Principle 6: Patient Privacy Rights

Basic Privacy and Security Principles

Stanford HEALTH CARE

Introduction

As you go about your duties for Stanford, there are six basic privacy principles that will help guide your thoughts and actions. Each of us makes decisions every day about how we use PHI for our jobs, how we release PHI to others, what PHI we access and how we communicate PHI with patients and others. Patient privacy laws and rules are complex and there is much to remember. Keeping these six guiding principles top-of-mind in your daily work will help you know what to do and make the right decisions about protecting patient privacy.

Later in this training, practical examples will be given about how these six guiding principles apply to the work that you do. In this section, you will focus on understanding the meaning behind the six guiding principles.

The six patient privacy guiding principles that you should understand and that you should think about every day in your role of protecting patient privacy are:

Principle 1: Minimum Necessary
Principle 2: Need to Know
Principle 3: Authorized Uses and Disclosures
Principle 4: Verification
Principle 5: Safeguards
Principle 6: Patient Privacy Rights

Basic Privacy and Security Principles

Stanford HEALTH CARE

Principle 1: Minimum Necessary

Patient privacy laws and our privacy policies require that you actively make a determination about what is the minimum amount of patient information that you need for each and every internal use or external disclosure that you do, as well as for every time that you access patient information in patient or research data systems. The minimum necessary principle applies to your conversations about patients as well. You are expected to actively consider what patient information is needed for a given purpose, and to use or disclose only the minimum necessary information. When you need patient information from others, you are required to request only the minimum amount of patient information that you need.

The minimum necessary principle also means that you question others when they ask you for information that seems inappropriate so that you can determine the minimum necessary information that you should release to them, including whether they need any patient information at all. You should be especially cautious before using or disclosing the entire medical record, or when using or disclosing patient names, social security numbers, credit card or bank account numbers, medical record numbers, dates of service or birthdates, and patient contact information. If you work at the

‹ PREV

Basic Privacy and Security Principles

Stanford HEALTH CARE

Principle 1: Minimum Necessary

dates of service or birthdates, and patient contact information. If you work at the School of Medicine, social security numbers, credit card numbers and bank account numbers are considered Prohibited Information. If your job requires you to use or disclose any of this information, you must have approval from the data governance board before you begin your work. Your supervisor or manager can confirm that you have the necessary approvals required for these activities.

It is important to remember that the privacy laws were never intended to interfere with patient care. Information needed to treat a patient should flow freely among the members of the treatment team. Generally, the minimum necessary information for treatment purposes is everything needed by the treatment team to provide care for the patient.

An important concept under the minimum necessary principle is the concept of de-identified information. Your first thought when using or disclosing patient information should be whether de-identified information would do for the intended purpose. You

PREV

Basic Privacy and Security Principles

Stanford HEALTH CARE

Principle 1: Minimum Necessary

are required to use and disclose de-identified information whenever possible. Using more than de-identified information when you reasonably could have used de-identified information for the task-at-hand is a violation of privacy law and of our policies.

De-identified information is specifically defined under the law. Many of us think that we have de-identified patient information when in fact it is not de-identified under the law. To qualify as de-identified information under the law, you must not include any of the following patient identifiers, alone or in combination with other information.

If any one of the following identifiers is included in the information that you use or disclose, it is not considered de-identified.

- Names;
- Social Security numbers;
- Telephone numbers;
- Addresses and all geographic subdivisions smaller than a state;
- All elements of dates (except year), including birth date, admission date.

‹ PREV

Basic Privacy and Security Principles

Stanford HEALTH CARE

Principle 1: Minimum Necessary

- All elements of dates (except year), including birth date, admission date, discharge date, date of death; and all ages over 89;
- Fax numbers;
- Electronic mail (e-mail addresses);
- Medical Record numbers;
- Health Plan Beneficiary numbers;
- Account numbers;
- Certificate/license numbers;
- Vehicle identifiers and serial numbers, including license plate numbers;
- Device identifiers and serial numbers;
- Web Universal Resource Locators (URLs);
- Internet Protocol (IP) addresses;
- Biometric Identifiers, including finger and voice prints;
- Full face photographic images and any comparable images; and
- Any other unique identifying number, characteristic or code.

Remember that "any other unique identifying number, characteristic or code" is a broad term that includes any unique patient information that could be used to identify

< PREV

Principle 1: Minimum Necessary

Remember that "any other unique identifying number, characteristic or code" is a broad term that includes any unique patient information that could be used to identify the patient and that there is no actual knowledge that the information could be used to identify the patient.

Using and disclosing de-identified information whenever possible will help protect our patients, Stanford and you from privacy breaches. If using or disclosing de-identified information for the intended purpose is not possible, you should ask yourself whether using or disclosing just dates (such as date of service or birth date) or geographic areas smaller than a state (such as zip codes or counties) would do. Using or disclosing just dates or geographic areas falls within a concept under the law known as a "limited data set" and there are certain limited protections regarding privacy breaches when you use or disclose a limited data set. A limited data set is not the same as de-identified information and using or disclosing a limited data set can result in a violation of the law if de-identified information could have been used, or could result in a privacy breach if the limited data set were used or disclosed inappropriately. Uses and disclosures of a limited data set require a special written agreement between the parties exchanging the limited data set. Contact your Privacy Office for more information about using or disclosing a limited data set.

Basic Privacy and Security Principles

Stanford HEALTH CARE

Principle 2: Need to Know

You are permitted only to access, use or disclose patient information when you have a job-related need to know. If you do not need patient information to perform a specific job function for Stanford, then the privacy laws prohibit you from accessing the information, internally using the information, or disclosing the information outside of Stanford.

Accessing patient information out of curiosity, or because you are concerned about a co-worker or friend, or because you want to study certain records for your own benefit are not legitimate job-related purposes. If the information is not specifically required for you to do your job at Stanford, then you do not have a job-related need to know.

The Privacy Offices monitor electronic medical records (Epic, Cerner or STRIDE) and can detect inappropriate access to patient records. Every section of the electronic medical record that you view and every click that you make in the system create an audit log for you. The SCH/SHC Privacy Office conducts access audits by patient (to see who has accessed any given patient's record) and by individuals who log into the system (to see all the records any given individual has accessed), and uses this information to conduct evaluations of whether any given access to any given record

< PREV

Basic Privacy and Security Principles

Stanford HEALTH CARE

Principle 2: Need to Know

specific job function for Stanford, then the privacy laws prohibit you from accessing the information, internally using the information, or disclosing the information outside of Stanford.

Accessing patient information out of curiosity, or because you are concerned about a co-worker or friend, or because you want to study certain records for your own benefit are not legitimate job-related purposes. If the information is not specifically required for you to do your job at Stanford, then you do not have a job-related need to know.

The Privacy Offices monitor electronic medical records (Epic, Cerner or STRIDE) and can detect inappropriate access to patient records. Every section of the electronic medical record that you view and every click that you make in the system create an audit log for you. The SCH/SHC Privacy Office conducts access audits by patient (to see who has accessed any given patient's record) and by individuals who log into the system (to see all the records any given individual has accessed), and uses this information to conduct evaluations of whether any given access to any given record meets the need-to-know principle. Stanford employees have been terminated for accessing electronic medical records without a job-related need to know.

‹ PREV

Basic Privacy and Security Principles

Stanford HEALTH CARE

Principle 3: Authorized Uses and Disclosures

Introduction

Accessing, using or disclosing patient information must be authorized. Authorized use and disclosure of PHI can occur in two ways; the use or disclosure of PHI is authorized by state or federal law, or it is authorized by the patient. Any other use or disclosure that is not authorized specifically by the patient or the law is considered unauthorized and would be a violation of the law and of Stanford policies. Accessing PHI in our computer systems is considered an internal use of PHI.

Use or Disclosure of PHI Authorized by State or Federal Privacy Law:

State and federal laws authorize the use or disclosure of PHI for certain purposes, meaning that the laws permit or require specific uses or disclosures of PHI for specific purposes. It is important to understand that the principle of authorized use and disclosure depends on the purpose of the use or disclosure, not on who the Stanford person is who may be using or disclosing. For instance, a clinician is not authorized to use PHI for any purpose just because he is a clinician, but only for purposes that are authorized by the law or by the patient. When you apply the principle of authorized use and disclosure in your daily work, you should focus on the purpose of the use or disclosure.

Basic Privacy and Security Principles

Stanford HEALTH CARE

Principle 3: Authorized Uses and Disclosures

The most common purpose for using or disclosing PHI that is authorized by law is for treatment purposes. This would include sharing information with non-Stanford physicians and other hospitals that are involved in a patient's care. Another common authorized purpose is using and disclosing PHI for Stanford payment purposes, including payment for faculty professional services. The law authorizes the use and disclosure of PHI for the purposes of operating Stanford business functions that support treatment and payment, such as administrative, financial, legal, or quality improvement purposes. There are rules that limit the sharing of PHI with other organizations for their payment purposes or their business operations purposes. Contact the Privacy Offices if you need advice regarding sharing PHI with other organizations for their payment or business operations purposes.

Uses and disclosures of PHI that are required by various federal and state laws are also authorized by the privacy laws, such as mandatory disclosures to state agencies related to births, deaths, disease tracking, FDA regulated products, and child abuse or neglect. Uses and disclosures of PHI to state or federal agencies authorized to receive PHI for health oversight purposes and public health purposes are considered authorized under the privacy laws. Also authorized under the privacy laws are certain, but not all, uses and disclosures related to law enforcement and judicial proceedings.

‹ PREV

Principle 3: Authorized Uses and Disclosures

authorized under the privacy laws. Also authorized under the privacy laws are certain, but not all, uses and disclosures related to law enforcement and judicial proceedings. If you are not certain whether a specific use or disclosure of this nature is authorized under the privacy laws, you should contact your Privacy Office for guidance.

Use and disclosure of PHI for research purposes is authorized by privacy law, but is subject to a complex set of requirements. Contact the University Privacy Office if you need assistance in using or disclosing PHI for human subject research purposes. If you are planning to conduct medical record research (including records of deceased patients), billing data or other data research, or engage in activities preparatory to human subject research, please contact the Stanford Privacy Offices for approval.

Keep in mind that the Minimum Necessary principle and the Need-to-Know principle apply when using and disclosing PHI for any of these purposes that are authorized by privacy law.

Use or Disclosure of PHI Authorized by the Patient:

Basic Privacy and Security Principles

Stanford HEALTH CARE

Principle 3: Authorized Uses and Disclosures

Use or Disclosure of PHI Authorized by the Patient:

Patients can authorize specific uses or disclosures of their PHI that would not otherwise be permitted under the privacy laws through a formal, written authorization process. When patient authorization is required under the law, verbal authorizations are not valid, except in certain research cases as approved by the Stanford University Institutional Review Board (IRB). Privacy laws require specific content and statements in order for a written authorization to be valid, as well as patient or legal guardian signature. Stanford has an approved authorization template that includes all the required elements of a valid authorization. Written and signed patient authorizations at the hospital must be filed with the Health Information Management Services Department (HIMS) and scanned into the medical record before any action can be taken related to the authorization. Any patient authorization that is not the SCH/SHC template must be reviewed and approved by HIMS before any action is taken in accordance with the patient authorization. The PHI that can be used or disclosed under a patient authorization must be limited to the PHI that is expressly described in the authorization. Care must be taken not to use or disclose additional information.

Basic Privacy and Security Principles

Stanford HEALTH CARE

Principle 3: Authorized Uses and Disclosures

Written and signed research participants' authorizations must be kept on file by the study's Principal Investigator. Any research participant authorization that is not on the Stanford Research Authorization template must be reviewed and approved by the University Privacy Office and the IRB before any action is taken in accordance with the authorization.

Special Considerations for Use and Disclosure of PHI

Special rules apply to the use and disclosure of especially sensitive PHI such as HIV test results, family planning services, mental health services, hereditary disorders, and services or research involving all aspects of genetic testing, counseling and education. Contact your Privacy Office if you need advice regarding using or disclosing PHI when this type of sensitive information is involved.

Direct or indirect remuneration from a third party (including gifts, fees, payments, subsidies, or other tangible or intangible benefit) in exchange for or related to the use or disclosure of PHI is prohibited without authorization from the patient. Even if the access, use or disclosure of PHI is for communications related to a patient's health care or about a health-related product or service, patient authorization must be

PREV

Basic Privacy and Security Principles

Stanford HEALTH CARE

Principle 3: Authorized Uses and Disclosures

care or about a health-related product or service, patient authorization must be obtained if direct or indirect remuneration will be received. The authorization must inform patients that direct or indirect remuneration will be received from the use or disclosure of PHI. Contact your Privacy Office if you need advice regarding the use or disclosure of PHI for activities that might be considered marketing or that might involve direct or indirect remuneration.

Any research participant authorization that is not on the Stanford Research Authorization template must be reviewed and approved by the University Privacy Office and the IRB before any action is taken in accordance with the authorization.

Business Associates:

The privacy laws permit us to engage business associates, such as vendors or consultants, to help us with our work that involves PHI. If you engage a business associate for SCH or SHC, you must have a formal written business associate agreement in place and on file with the Contracting Office in the SCH/SHC Materials Management Department before any PHI can be exchanged with the business

< PREV

Principle 3: Authorized Uses and Disclosures

agreement in place and on file with the Contracting Office in the SCH/SHC Materials Management Department before any PHI can be exchanged with the business associate. You must use the official SCH/SHC business associate agreement template, unless approval is obtained from the Contracting Office to use a different business associate agreement. You should contact the Contracting Office for guidance related to the required agreement.

If you want to engage a business associate for the School of Medicine or Stanford University, you must first submit a request (requisition) to Stanford Procurement Services to issue a contract, even if the contract value is less than $25,000. Make sure that you indicate on the requisition that the supplier will have access to PHI to ensure that Procurement Services includes a business associate agreement as part of the contract. You should contact Stanford Procurement Services for guidance related to the required agreement.

There are many requirements imposed upon Business Associates. Never sign an agreement that would make you, your department or Stanford a business associate of another organization without first contacting the Stanford Privacy Offices.

Principle 3: Authorized Uses and Disclosures

another organization without first contacting the Stanford Privacy Offices.

If an electronic sharing of PHI with a business associate is contemplated, you must contact the appropriate Stanford IT Security Office so that they can conduct a security review of the business associate before you sign a contract for services with the business associate. The business associate must not be permitted to send PHI to offshore entities, or permit access to PHI from offshore entities, without the express approval of the appropriate Privacy Office and IT Security Office.

It is important to remember that the Minimum Necessary and Need-to-Know principles strictly apply when sharing PHI with business associates. Additionally, it is important to remember that sharing PHI with business associates is subject to the same principle of authorized use and disclosure in that the PHI shared with a business associate must be authorized by privacy law or authorized by a patient. A business associate agreement is not a substitute for patient authorization when patient authorization is required.

If you engage a business associate to assist with Stanford business, you are responsible for ensuring that the business associate is following the same privacy

Basic Privacy and Security Principles

Stanford HEALTH CARE

Principle 3: Authorized Uses and Disclosures

important to remember that sharing PHI with business associates is subject to the same principle of authorized use and disclosure in that the PHI shared with a business associate must be authorized by privacy law or authorized by a patient. A business associate agreement is not a substitute for patient authorization when patient authorization is required.

If you engage a business associate to assist with Stanford business, you are responsible for ensuring that the business associate is following the same privacy standards that Stanford must follow. You are responsible for knowing whether the business associate is using subcontractors or sharing the PHI with any other individual or entity.

You are expected to actively manage the relationship between Stanford and the business associate on an ongoing basis, and to routinely have conversations with the business associate about the security of the PHI that you entrust to them. You are responsible for terminating the business associate's access to Stanford systems when your contract expires, and for knowing when an individual who works for the business associate no longer needs access to PHI and immediately terminating that individual's access.

< PREV

Basic Privacy and Security Principles

Stanford HEALTH CARE

Principle 4: Verification

Patient privacy laws and our policies require verification procedures when PHI is requested of us, or when communicating or releasing PHI to others. If it is part of your job to receive inquiries about patients from individuals, or to communicate PHI to individuals, you must verify both the identity of the person and his or her authority to have the information requested before responding to the request or communicating the PHI.

Verifying the identity means that you are taking reasonable steps to establish that the person is who they say they are. If someone other than the patient is requesting information about the patient over the phone or in person, you are required to establish his or her authority to receive the requested information. Verifying the identity of the person requesting information from you or the person to whom you will be releasing PHI and verifying the person's authority to receive the information means that you ask questions to reasonably establish that the person is who they say they are and that they are authorized to have the PHI requested or to receive the PHI that you need to communicate.

Basic Privacy and Security Principles

Stanford HEALTH CARE

Principle 5: Safeguards

Privacy laws require that we safeguard PHI in any form - physical form such as paper records and notes or verbal form such as conversations, as well as electronic form such as in our IT systems and accessed through our computers. PHI in electronic form is known as ePHI. Each of us must take precautionary measures to protect PHI and ePHI in everything we do. This requires proactive actions on your part as you go about your daily routine. Principles related to safeguarding PHI include:

- Access control
- Remote access
- Workstation security
- Safe handling and storage of ePHI
- Secure email
- Secure external data transfers
- Secure Smartphones, tablets, laptops and other computing devices
- Use and disposal of computers and portable media
- Physical safeguards
- Acceptable Internet use
- Monitoring

Basic Privacy and Security Principles

Stanford HEALTH CARE

Principle 5: Safeguards *(continued)*

Click the **red** number to advance and scroll down to click Close after you have finished reading to learn about the specific safeguards in place to protect PHI.

Basic Privacy and Security Principles

Stanford HEALTH CARE

Principle 5: Safeguards *(continued)*

Click the **red** number to advance and scroll down to click Close after you have finished reading to learn about the specific safeguards in place to protect PHI.

Access Control

There are many different information systems within Stanford. Requests to get access to data must be based on Stanford business needs and must be reasonably limited to the data you need to do your job for Stanford. Your manager will determine which systems you need to access. If you supervise individuals who access PHI, you must ensure that the access is appropriate for their job roles and is kept up-to-date. As a supervisor, it is your responsibility to change or terminate the individual's access to IT systems that contain PHI when the individual changes job functions, leaves Stanford, or the scope of PHI accessed is no longer appropriate for the individual's role at Stanford.

You are required to keep your IT system login IDs and passwords confidential and must

DONE

Basic Privacy and Security Principles

Stanford HEALTH CARE

Principle 5: Safeguards *(continued)*

Click the red number to advance and scroll down to click Close after you have finished reading to learn about the specific safeguards in place to protect PHI.

1 2 3 4 5 6 7 8 9 10 11

when the individual changes job functions, leaves Stanford, or the scope of PHI accessed is no longer appropriate for the individual's role at Stanford.

You are required to keep your IT system login IDs and passwords confidential and must never share your password with anyone else. Any access to ePHI that occurs under your login ID and password is your responsibility. It is never permissible to ask others to provide you with their username or password. You must log off applications, "lock" your computer, or otherwise secure your computer whenever you walk away from your computer. You will be held accountable for any access that occurs under your username and password, even if it occurred because you failed to log off the application or lock the computer. You are required to choose strong passwords. You must use a minimum of 8 characters for any of your passwords and should use longer ones whenever possible.

DONE

Basic Privacy and Security Principles

Principle 5: Safeguards *(continued)*

Click the **red** number to advance and scroll down to click Close after you have finished reading to learn about the specific safeguards in place to protect PHI.

Remote Access

Stanford has secure remote access solutions that allow you to work off site, such as from home or locations outside Stanford. These secure remote access solutions can minimize the need for you to carry around paper documents, notes and files, as well as walking with external storage devices such as USB drives (also known as flash drives or thumb drives) and external hard drives.

You must have approval from your supervisor to conduct work off site that includes PHI and you must contact your hospital IT Security Department or the School of Medicine's IT Support to determine the appropriate Stanford remote access solution for your business needs.

Basic Privacy and Security Principles

Stanford HEALTH CARE

Principle 5: Safeguards *(continued)*

Click the **red** number to advance and scroll down to click Close after you have finished reading to learn about the specific safeguards in place to protect PHI.

1 2 3 4 5 6 7 8 9 10 11

Workstation Security

SCH and SHC computer workstations have an approved software image installed as part of initial computer configuration. SCH/SHC workstations are updated regularly by the IT Department to install new versions of software, fix problems and update security settings. All software must be approved and installed by an SCH/SHC IT Department Technician and you are not permitted to download or otherwise install software without permission from the IT Department. Never save ePHI on your workstation computer's hard disk drive ("C:" or "Desktop" locations).

School of Medicine and Stanford University computers that are used to access, transmit and store ePHI must also be configured in an approved manner. This includes having backup, whole disk encryption, passwords and auto-lock properly installed and configured. Your IT support team can assist in ensuring your computer is compliant with the requirements to store ePHI.

Basic Privacy and Security Principles

Stanford HEALTH CARE

Principle 5: Safeguards *(continued)*

Click the **red** number to advance and scroll down to click Close after you have finished reading to learn about the specific safeguards in place to protect PHI.

not permitted to download or otherwise install software without permission from the IT Department. Never save ePHI on your workstation computer's hard disk drive ("C:" or "Desktop" locations).

School of Medicine and Stanford University computers that are used to access, transmit and store ePHI must also be configured in an approved manner. This includes having backup, whole disk encryption, passwords and auto-lock properly installed and configured. Your IT support team can assist in ensuring your computer is compliant with the requirements to store ePHI.

All computers that access ePHI should have their screens positioned so that information on display is not easily viewable by others, particularly workstations in public areas.

Basic Privacy and Security Principles

Stanford HEALTH CARE

Principle 5: Safeguards *(continued)*

Click the **red** number to advance and scroll down to click Close after you have finished reading to learn about the specific safeguards in place to protect PHI.

Safe Handling and Storage of ePHI

When using an SCH/SHC workstation, all work files and documents with ePHI must be stored on SCH/SHC network servers or a shared drive on the SCH/SHC trusted network, unless you have specific approval from the SCH or SHC IT Security Department to store or "save" ePHI elsewhere. ePHI must be stored in secure electronic locations that meet SCH/SHC security standards and must never be stored or saved to external drives, USB drives, other removable devices, or cloud solutions without first contacting the IT Security Office for approval.

The SCH/SHC IT Security Office will evaluate your business need and determine the most appropriate way for you to save or transport ePHI. All files and documents with ePHI must be stored on an approved encrypted storage device.

Basic Privacy and Security Principles

Stanford HEALTH CARE

Principle 5: Safeguards *(continued)*

Click the **red** number to advance and scroll down to click Close after you have finished reading to learn about the specific safeguards in place to protect PHI.

ePHI should never be stored on unencrypted hard drives, external drives, USB drives, or other removable devices.

There are serious privacy concerns associated with the use of Cloud or Web storage, file sharing, or data conversion solutions. Do not use such solutions for ePHI unless the solution is specifically approved for use with ePHI and this has been confirmed by your IT support. Other solutions must be specifically approved by Stanford. Stanford IT Departments have engineered secure solutions to meet your business needs when handling ePHI. You are not permitted to independently use Cloud-based or Internet-based data storage or sharing solutions with ePHI.

Basic Privacy and Security Principles

Stanford HEALTH CARE

Principle 5: Safeguards *(continued)*

Click the **red** number to advance and scroll down to click Close after you have finished reading to learn about the specific safeguards in place to protect PHI.

Secure Email, Instant Messaging and Text Messaging

All messages sent and received on your "SCH.org", "stanfordmed.org", "stanfordhealthcare.org" or "stanford.edu" email accounts are the property of Stanford and are not your personal property, even if you send occasional personal emails during your break time.

Email that contains ePHI, either in the body of the email or as an attachment to an email, must be sent securely via your "SCH.org", "stanfordmed.org", "stanfordhealthcare.org" or "stanford.edu" email accounts, or via the secure patient communication systems such as Epic MyHealth or Cerner IQHealth. Do not use personal accounts to send messages to patients. Do not give your personal address or screen name to patients or their families to communicate with you. Sometimes patients find our personal addresses on their own and send messages to those personal accounts. If you receive a message from a patient on your

< PREV

Principle 5: Safeguards *(continued)*

Click the **red** number to advance and scroll down to click Close after you have finished reading to learn about the specific safeguards in place to protect PHI.

send messages to those personal accounts. If you receive a message from a patient on your personal account, use your "SCH.org", "stanfordmed.org", "stanfordhealthcare.org" or "stanford.edu" email account to respond to the patient. Personal email accounts should not be used to conduct Stanford business. You should never forward your Stanford email to your personal email account.

You must type "secure:" (the word - secure - with a colon after it) in the subject line of all emails that contain ePHI in the body of the email or in an attachment to the email. You must type "secure:" in the subject line of any email that contains one or more of the elements that were described in this training under "Section 1: Information Protected Under the Law." It is important to remember that the subject line of an email is not encrypted and you must never include ePHI in the subject line itself.

If you send a "secure:" email to someone outside Stanford, such as a patient, they will

Basic Privacy and Security Principles

Stanford HEALTH CARE

Principle 5: Safeguards *(continued)*

Click the **red** number to advance and scroll down to click Close after you have finished reading to learn about the specific safeguards in place to protect PHI.

You must type "secure:" (the word - secure - with a colon after it) in the subject line of all emails that contain ePHI in the body of the email or in an attachment to the email. You must type "secure:" in the subject line of any email that contains one or more of the elements that were described in this training under "Section 1: Information Protected Under the Law." It is important to remember that the subject line of an email is not encrypted and you must never include ePHI in the subject line itself.

If you send a "secure:" email to someone outside Stanford, such as a patient, they will receive an email message instructing them how to open the secure email as an attachment. The message also explains that if this is the first time they have received a "secure:" email, they will need to register with the secure email system, but only the first time they receive a "secure:" message. After that, they will simply be instructed to open the attachment containing your encrypted email.

Basic Privacy and Security Principles

Stanford HEALTH CARE

Principle 5: Safeguards *(continued)*

Click the **red** number to advance and scroll down to click Close after you have finished reading to learn about the specific safeguards in place to protect PHI.

External Data Transfers

Stanford has systems and procedures in place to ensure that transmitting ePHI outside the organization and receiving ePHI from external sources occur in a secure manner. All data transmissions and electronic file transfers containing ePHI must be encrypted using a Stanford approved system protocol or algorithm. Only individuals whose job functions authorize them to transmit data or files with ePHI are permitted to do so. Stanford IT Security groups will provide assistance for setting up secure procedures for ePHI data transfers for departments and individuals and you are required to obtain IT Security Department approval regarding secure methods for ePHI data transfer before external data transfers occur. Requests to move data from one source to another must be approved in writing by the data owner or the business owner for the system or application.

Any identifiable data to be used for research must be approved by the Stanford University Institutional Review Board (IRB) and the data requester must be prepared to submit specific

‹ PREV

Basic Privacy and Security Principles

Stanford HEALTH CARE

Principle 5: Safeguards *(continued)*

Click the **red** number to advance and scroll down to click Close after you have finished reading to learn about the specific safeguards in place to protect PHI.

External Data Transfers

Stanford has systems and procedures in place to ensure that transmitting ePHI outside the organization and receiving ePHI from external sources occur in a secure manner. All data transmissions and electronic file transfers containing ePHI must be encrypted using a Stanford approved system protocol or algorithm. Only individuals whose job functions authorize them to transmit data or files with ePHI are permitted to do so. Stanford IT Security groups will provide assistance for setting up secure procedures for ePHI data transfers for departments and individuals and you are required to obtain IT Security Department approval regarding secure methods for ePHI data transfer before external data transfers occur. Requests to move data from one source to another must be approved in writing by the data owner or the business owner for the system or application.

Any identifiable data to be used for research must be approved by the Stanford University Institutional Review Board (IRB) and the data requester must be prepared to submit specific paperwork demonstrating proper approval.

‹ PREV

Basic Privacy and Security Principles

Stanford HEALTH CARE

Principle 5: Safeguards *(continued)*

Click the **red** number to advance and scroll down to click Close after you have finished reading to learn about the specific safeguards in place to protect PHI.

1 2 3 4 5 6 7 8 9 10 11

Smartphones, tablets, laptops and other mobile computing devices:

Using laptops, iPads and other tablets, cell phones, smartphones, and other mobile devices to handle ePHI poses significant risk of loss or theft. If you use such devices to send or receive ePHI, to access ePHI in Stanford systems, or to otherwise handle ePHI, you are required to ensure that the device has adequate safeguards installed and activated that meet or exceed Stanford security settings, such as encryption, password protection and remote data wipe capability. Additionally, you must be prepared to demonstrate business need and approval (from supervisor and data owner) for using these types of mobile devices for the storage of ePHI.

If you have an "SCH.org" or a "stanfordmed.org" email address and you want to synchronize your email to your personal mobile device, you must contact the SCH or SHC IT Security Department to ensure that your device meets security configuration requirements. If you have a

< PREV

Basic Privacy and Security Principles

Stanford HEALTH CARE

Principle 5: Safeguards *(continued)*

Click the **red** number to advance and scroll down to click Close after you have finished reading to learn about the specific safeguards in place to protect PHI.

remote data wipe capability. Additionally, you must be prepared to demonstrate business need and approval (from supervisor and data owner) for using these types of mobile devices for the storage of ePHI.

If you have an "SCH.org" or a "stanfordmed.org" email address and you want to synchronize your email to your personal mobile device, you must contact the SCH or SHC IT Security Department to ensure that your device meets security configuration requirements. If you have a "stanford.edu" email address, contact the Stanford University IT Helpdesk. You must have permission from your supervisor to use any mobile device to handle ePHI.

If you use a personal smartphone, tablet, laptop or other personal mobile computing device to send, receive, access or otherwise handle ePHI, you must implement and abide by the specific safeguard requirements that are outlined in the next section of this training. Failure to do so may result in disciplinary action, up to and including termination. If ePHI under your control is misused, lost, stolen or otherwise inappropriately accessed, serious consequences may also apply to you individually.

< PREV

Basic Privacy and Security Principles

Stanford HEALTH CARE

Principle 5: Safeguards *(continued)*

Click the **red** number to advance and scroll down to click Close after you have finished reading to learn about the specific safeguards in place to protect PHI.

Use and Disposal of Computers and Portable Media:

Only approved devices may be connected to hospital systems. Approved devices include computers, laptops and other devices that have been issued by the SCH or SHC IT Department. Personal laptops and portable media, such as external drives and flash drives that are not issued by the IT Department, may not be connected to SCH or SHC systems without pre-approval of the SCH/SHC IT Department.

Devices and equipment that are no longer needed and that contain ePHI must undergo special cleansing or destruction procedures. It is not enough to simply delete the data off the device or equipment when you no longer need the device or equipment. Assume that any Stanford-issued computer, laptop, tablet, fax, copier or piece of clinical equipment contains ePHI, and upon retirement must be destroyed in accordance with the SCH, SHC or School of Medicine's IT Department procedures for safe destruction of ePHI.

School of Medicine and Stanford University devices that may have unencrypted ePHI (cameras,

< PREV

Basic Privacy and Security Principles

Stanford HEALTH CARE

Principle 5: Safeguards *(continued)*

Click the **red** number to advance and scroll down to click Close after you have finished reading to learn about the specific safeguards in place to protect PHI.

1 2 3 4 5 6 7 8 9 10 11

approval of the SCH/SHC IT Department.

Devices and equipment that are no longer needed and that contain ePHI must undergo special cleansing or destruction procedures. It is not enough to simply delete the data off the device or equipment when you no longer need the device or equipment. Assume that any Stanford-issued computer, laptop, tablet, fax, copier or piece of clinical equipment contains ePHI, and upon retirement must be destroyed in accordance with the SCH, SHC or School of Medicine's IT Department procedures for safe destruction of ePHI.

School of Medicine and Stanford University devices that may have unencrypted ePHI (cameras, servers, fax machines, copiers, etc.) must be disposed of properly. Work with your Department Property Administrator (DPA) to ensure the memory and storage devices are properly cleansed or destroyed before the device is disposed of. Any device being reissued to another user must be reset to factory defaults by IT before it can be reused.

PREV

Basic Privacy and Security Principles

Stanford HEALTH CARE

Principle 5: Safeguards *(continued)*

Click the **red** number to advance and scroll down to click Close after you have finished reading to learn about the specific safeguards in place to protect PHI.

Physical Safeguards:

When you are transporting PHI or ePHI, you are required to have it in your possession and under your control at all times. Never leave papers or devices with PHI out of your personal possession, even for a minute. Keep them physically with you at all times. It is not acceptable to lay down a backpack or briefcase while you wait for a train, are seated at a restaurant or stand in line. It is not acceptable to leave papers or devices in your car, even in a locked trunk, even in your garage.

If you have permission to work from home, you must lock up papers or devices that contain PHI. You are required to immediately report missing papers or devices to the Stanford Privacy Offices. You are responsible for knowing exactly what PHI you have or had in your possession, and for being able to describe every detail of PHI to the Privacy Office in the event of missing, lost or stolen papers or devices.

All paper documents with PHI, from medical records to notes you take about patients, must be

PREV

Principle 5: Safeguards *(continued)*

Click the **red** number to advance and scroll down to click Close after you have finished reading to learn about the specific safeguards in place to protect PHI.

possession, even for a minute. Keep them physically with you at all times. It is not acceptable to lay down a backpack or briefcase while you wait for a train, are seated at a restaurant or stand in line. It is not acceptable to leave papers or devices in your car, even in a locked trunk, even in your garage.

If you have permission to work from home, you must lock up papers or devices that contain PHI. You are required to immediately report missing papers or devices to the Stanford Privacy Offices. You are responsible for knowing exactly what PHI you have or had in your possession, and for being able to describe every detail of PHI to the Privacy Office in the event of missing, lost or stolen papers or devices.

All paper documents with PHI, from medical records to notes you take about patients, must be disposed of in Stanford secure shred bins when no longer needed.

Basic Privacy and Security Principles

Stanford HEALTH CARE

Principle 5: Safeguards *(continued)*

Click the **red** number to advance and scroll down to click Close after you have finished reading to learn about the specific safeguards in place to protect PHI.

Acceptable Internet Use:

A tremendous amount of IT resources go into protecting Stanford networks and systems from intrusions and malicious attacks. As a user of these networks and systems, you play an important role in helping to keep the data secure. Malware such as viruses, worms and spyware can infiltrate computer systems via Internet usage, such as when you download or install software or click on advertisement links or other unknown links that are sent to you in emails. Never download software from the Internet without approval from your IT support. On SCH/SHC workstations, all software must be approved and installed by a SCH or SHC IT technician. On School of Medicine or Stanford University workstations, have your IT support group obtain and install the software.

Never provide your login ID or password if you receive an email requesting them. Immediately forward such emails to "EmailAbuse@stanfordmed.org," "security@stanford.edu," or to the SCH Service Desk as appropriate. The Stanford IT Departments will never ask you for your

< PREV

Basic Privacy and Security Principles

Stanford HEALTH CARE

Principle 5: Safeguards *(continued)*

Click the **red** number to advance and scroll down to click Close after you have finished reading to learn about the specific safeguards in place to protect PHI.

can infiltrate computer systems via Internet usage, such as when you download or install software or click on advertisement links or other unknown links that are sent to you in emails. Never download software from the Internet without approval from your IT support. On SCH/SHC workstations, all software must be approved and installed by a SCH or SHC IT technician. On School of Medicine or Stanford University workstations, have your IT support group obtain and install the software.

Never provide your login ID or password if you receive an email requesting them. Immediately forward such emails to "EmailAbuse@stanfordmed.org," "security@stanford.edu," or to the SCH Service Desk as appropriate. The Stanford IT Departments will never ask you for your passwords. If you believe your computer has been compromised, received a virus, or if you suspect a malicious attack or intrusion of our IT systems, contact the SCH, SHC or School of Medicine IT Helpdesk immediately.

CLOSE

Basic Privacy and Security Principles

Principle 5: Safeguards *(continued)*

Click the **red** number to advance and scroll down to click Close after you have finished reading to learn about the specific safeguards in place to protect PHI.

Monitoring

Stanford has the right to monitor your email, your Internet use, and your access to systems. The SCH and SHC IT Security Departments conduct routine reviews of network activity for individuals as part of their security monitoring programs and can detect and block inappropriate access to Internet sites, such as pornographic websites and gambling websites, as well as the sending of ePHI to unapproved external sites, such as Gmail, Dropbox or Facebook. The SCH/SHC Privacy Office conducts routine reviews of access to systems that contain ePHI and can detect inappropriate access to patient information in these systems. The School of Medicine and University also have network monitoring programs.

Basic Privacy and Security Principles

Stanford HEALTH CARE

Principle 6: Patient Privacy Rights

Patient Privacy laws grant certain privacy rights to patients as part of their civil rights. Stanford is committed to assisting patients in exercising their privacy rights. Requirements for accommodating patient privacy rights are complex and often involve timelines for response. Assisting patients with their privacy rights must be done under the guidance of the SCH/SHC Privacy Office or the hospital Health Information Management Services (HIMS) Department.

Use the scroll bar to learn more about patients' privacy rights. Click the **DONE** button when you have read all of the rights.

Patient privacy rights include:

- The right to receive a notice of Stanford privacy practices
- The right to see their medical and billing records and receive a copy of them
- The right to request an update to their medical record
- The right to receive an accounting of certain disclosures that we have made
- The right to select how they will receive their PHI from us
- The right to request restrictions on certain uses and disclosures of their PHI
- The right to express concerns or file a complaint about our privacy practices
- The right to be notified in the event of a privacy breach

Basic Privacy and Security Principles

Stanford HEALTH CARE

Principle 6: Patient Privacy Rights

Patient Privacy laws grant certain privacy rights to patients as part of their civil rights. Stanford is committed to assisting patients in exercising their privacy rights. Requirements for accommodating patient privacy rights are complex and often involve timelines for response. Assisting patients with their privacy rights must be done under the guidance of the SCH/SHC Privacy Office or the hospital Health Information Management Services (HIMS) Department.

Use the scroll bar to learn more about patients' privacy rights. Click the **DONE** button when you have read all of the rights.

1. Right to Receive a Notice of SCH/SHC Privacy Practices

Patient privacy laws require that we publish a Notice of Privacy Practices and patients have a right to receive a copy. Stanford's Notice of Privacy Practices is available on the SCH, SHC and University's Internet sites. Be certain that you are using the appropriate privacy notice for your organization.

2. Right to See Their Medical and Billing Records and Receive a Copy of Them

Patients have a right to read their medical record or their billing record and to receive a copy of their record in paper or electronic format. Under certain conditions, we can

Basic Privacy and Security Principles

Stanford HEALTH CARE

Principle 6: Patient Privacy Rights

Patient Privacy laws grant certain privacy rights to patients as part of their civil rights. Stanford is committed to assisting patients in exercising their privacy rights. Requirements for accommodating patient privacy rights are complex and often involve timelines for response. Assisting patients with their privacy rights must be done under the guidance of the SCH/SHC Privacy Office or the hospital Health Information Management Services (HIMS) Department.

Use the scroll bar to learn more about patients' privacy rights. Click the **DONE** button when you have read all of the rights.

Patients have a right to read their medical record or their billing record and to receive a copy of their record in paper or electronic format. Under certain conditions, we can deny the request, such as certain mental health records. If a patient requests a copy of their medical record, it is important that you refer them to the SCH or SHC HIMS Department. The HIMS Department is responsible for ensuring that medical records are released in accordance with state and federal privacy laws.

3. Right to Request an Update to Their Medical Record

If patients believe that a piece of important information is missing from their medical record, or that their medical record contains incorrect information, they have a right

< PREV

Basic Privacy and Security Principles

Stanford HEALTH CARE

Principle 6: Patient Privacy Rights

Patient Privacy laws grant certain privacy rights to patients as part of their civil rights. Stanford is committed to assisting patients in exercising their privacy rights. Requirements for accommodating patient privacy rights are complex and often involve timelines for response. Assisting patients with their privacy rights must be done under the guidance of the SCH/SHC Privacy Office or the hospital Health Information Management Services (HIMS) Department.

Use the scroll bar to learn more about patients' privacy rights. Click the **DONE** button when you have read all of the rights.

record, or that their medical record contains incorrect information, they have a right to request that we amend or add an addendum to their record. Under federal privacy law, patients have the right to request to amend or correct their medical records. Under certain conditions, we can deny such a request, such as if the information was not created by us or if we believe that the information is accurate and complete. Under state privacy law, patients have the right to add their own limited addendum to their medical record.

All requests for amendments or addendums to medical records must be managed by the HIMS Department. The HIMS Department, in collaboration with care providers, will

Basic Privacy and Security Principles

Stanford HEALTH CARE

Principle 6: Patient Privacy Rights

Patient Privacy laws grant certain privacy rights to patients as part of their civil rights. Stanford is committed to assisting patients in exercising their privacy rights. Requirements for accommodating patient privacy rights are complex and often involve timelines for response. Assisting patients with their privacy rights must be done under the guidance of the SCH/SHC Privacy Office or the hospital Health Information Management Services (HIMS) Department.

Use the scroll bar to learn more about patients' privacy rights. Click the **DONE** button when you have read all of the rights.

All requests for amendments or addendums to medical records must be managed by the HIMS Department. The HIMS Department, in collaboration with care providers, will make any amendments or addendums to medical records and will communicate with patients about their requests, as appropriate.

4. Right to Receive an Accounting of Certain Disclosures that We Have Made from Their Medical Record

Patients have a right to request a list of the certain disclosures that we have made of their PHI to outside parties. Disclosures that we make for purposes of treatment,

< PREV

Basic Privacy and Security Principles

Stanford HEALTH CARE

Principle 6: Patient Privacy Rights

Patient Privacy laws grant certain privacy rights to patients as part of their civil rights. Stanford is committed to assisting patients in exercising their privacy rights. Requirements for accommodating patient privacy rights are complex and often involve timelines for response. Assisting patients with their privacy rights must be done under the guidance of the SCH/SHC Privacy Office or the hospital Health Information Management Services (HIMS) Department.

Use the scroll bar to learn more about patients' privacy rights. Click the **DONE** button when you have read all of the rights.

their PHI to outside parties. Disclosures that we make for purposes of treatment, payment or healthcare operations do not need to be included in the accounting that we provide to the patients. Certain other disclosures must be included, such as disclosures made to state and federal agencies for health oversight or public health purposes and disclosures related to retrospective research studies. If a patient requests that you provide them with an accounting of disclosures, refer them to the SCH/SHC Privacy Office. The Privacy Office will compile the list of disclosures for the patient in accordance with state and federal privacy laws.

5. Right to Select How They Will Receive Their PHI from Us

< PREV

Basic Privacy and Security Principles

Stanford HEALTH CARE

Principle 6: Patient Privacy Rights

Patient Privacy laws grant certain privacy rights to patients as part of their civil rights. Stanford is committed to assisting patients in exercising their privacy rights. Requirements for accommodating patient privacy rights are complex and often involve timelines for response. Assisting patients with their privacy rights must be done under the guidance of the SCH/SHC Privacy Office or the hospital Health Information Management Services (HIMS) Department.

Use the scroll bar to learn more about patients' privacy rights. Click the **DONE** button when you have read all of the rights.

5. Right to Select How They Will Receive Their PHI from Us

Patients have the right to request confidential communications, meaning that they have a right to request that we communicate their PHI to them by an alternative method or at an alternative location. For example, a patient may request that we contact them only at work rather than at home, or that we email them rather than call them, or that we use a post office box rather than their home address. If you receive a patient request for alternative confidential communication, contact the SCH/SHC Privacy Office for guidance. Reasonable requests will be accommodated, but it is important to know that once we agree to an alternative method for communicating with the patient, we must all abide by it.

PREV

Basic Privacy and Security Principles

Stanford HEALTH CARE

Principle 6: Patient Privacy Rights

Patient Privacy laws grant certain privacy rights to patients as part of their civil rights. Stanford is committed to assisting patients in exercising their privacy rights. Requirements for accommodating patient privacy rights are complex and often involve timelines for response. Assisting patients with their privacy rights must be done under the guidance of the SCH/SHC Privacy Office or the hospital Health Information Management Services (HIMS) Department.

Use the scroll bar to learn more about patients' privacy rights. Click the **DONE** button when you have read all of the rights.

6. Right to Request Restrictions on Certain Uses and Disclosures of Their PHI

Patients have the right to request restrictions or limitations on how we use, disclose or communicate their PHI. In most cases, privacy laws do not require that we accept a patient's request to restrict our use or disclosure of their PHI, but it does require that each of us abides by the restriction if anyone in the organization accepts the restriction. If you receive a patient request that you restrict or limit how you use or disclose their PHI, contact the SCH/SHC Privacy Office for guidance. The Privacy Office will review the request and communicate with the patient in accordance with state and federal privacy laws.

Basic Privacy and Security Principles

Stanford HEALTH CARE

Principle 6: Patient Privacy Rights

Patient Privacy laws grant certain privacy rights to patients as part of their civil rights. Stanford is committed to assisting patients in exercising their privacy rights. Requirements for accommodating patient privacy rights are complex and often involve timelines for response. Assisting patients with their privacy rights must be done under the guidance of the SCH/SHC Privacy Office or the hospital Health Information Management Services (HIMS) Department.

Use the scroll bar to learn more about patients' privacy rights. Click the **DONE** button when you have read all of the rights.

In certain cases where a patient has paid out of pocket in full for a health care item or service and the patient has requested that we not bill or otherwise disclose PHI to the health plan, we must agree to the request. Contact your Privacy Office for assistance if unsure how to assist a patient in exercising this right.

Patients also have the right to opt-out of receiving fundraising or permitted marketing communications. When patients receive fundraising or permitted marketing communications, these communications will have clear and conspicuous language that provides patients with instructions on how they can opt-out from receiving future communications. Special attention must be paid to patient opt-out requests. Forward

Basic Privacy and Security Principles

Stanford HEALTH CARE

Principle 6: Patient Privacy Rights

Patient Privacy laws grant certain privacy rights to patients as part of their civil rights. Stanford is committed to assisting patients in exercising their privacy rights. Requirements for accommodating patient privacy rights are complex and often involve timelines for response. Assisting patients with their privacy rights must be done under the guidance of the SCH/SHC Privacy Office or the hospital Health Information Management Services (HIMS) Department.

Use the scroll bar to learn more about patients' privacy rights. Click the **DONE** button when you have read all of the rights.

communications. Special attention must be paid to patient opt-out requests. Forward these requests to your Privacy Office immediately.

7. Right to Express Concerns or File a Complaint about Our Privacy Practices

Patients have a right to file a complaint or express a concern about our privacy practices. If you receive a patient concern or complaint about privacy, immediately contact your Privacy Office and provide the contact information for the Privacy Office to the patient. The Privacy Office will assist the patient with their complaint or concern and will provide information about contacting state and federal authorities if the

Basic Privacy and Security Principles

Stanford HEALTH CARE

Principle 6: Patient Privacy Rights

Patient Privacy laws grant certain privacy rights to patients as part of their civil rights. Stanford is committed to assisting patients in exercising their privacy rights. Requirements for accommodating patient privacy rights are complex and often involve timelines for response. Assisting patients with their privacy rights must be done under the guidance of the SCH/SHC Privacy Office or the hospital Health Information Management Services (HIMS) Department.

Use the scroll bar to learn more about patients' privacy rights. Click the **DONE** button when you have read all of the rights.

and will provide information about contacting state and federal authorities if the patient wishes to file a complaint with such authorities.

8. Right to be notified in the event of a privacy breach

State and federal privacy laws require us to notify patients and research participants in the event of certain privacy breaches. Stanford's Privacy Offices will handle all privacy breach notifications. Never communicate independently with a patient about a potential or actual privacy breach. Contact your Privacy Office immediately if you are aware of a potential or possible privacy breach. The Privacy Office will notify patients

PREV

Basic Privacy and Security Principles

Stanford HEALTH CARE

Principle 6: Patient Privacy Rights

Patient Privacy laws grant certain privacy rights to patients as part of their civil rights. Stanford is committed to assisting patients in exercising their privacy rights. Requirements for accommodating patient privacy rights are complex and often involve timelines for response. Assisting patients with their privacy rights must be done under the guidance of the SCH/SHC Privacy Office or the hospital Health Information Management Services (HIMS) Department.

Use the scroll bar to learn more about patients' privacy rights. Click the **DONE** button when you have read all of the rights.

patient wishes to file a complaint with such authorities.

8. Right to be notified in the event of a privacy breach

State and federal privacy laws require us to notify patients and research participants in the event of certain privacy breaches. Stanford's Privacy Offices will handle all privacy breach notifications. Never communicate independently with a patient about a potential or actual privacy breach. Contact your Privacy Office immediately if you are aware of a potential or possible privacy breach. The Privacy Office will notify patients when needed in accordance with state and federal privacy laws.

PREV

Basic Privacy and Security Principles

Stanford HEALTH CARE

Section 3

Applying Privacy Principles to Your Everyday Work

Basic Privacy and Security Principles

Stanford HEALTH CARE

Introduction

In this section of training, you will focus on understanding the application of the basic privacy principles to your work. This section includes examples and rules to help guide you in your everyday practices. Many instances in addition to those described in this section will require you to apply the guiding principles found throughout this training.

Basic Privacy and Security Principles

Stanford HEALTH CARE

Section 3.1: Conversations

As you go about your daily routine, remember to:

- Keep voices down to a reasonable level
- Assess surroundings:
  - If you are in a public area such as a waiting room, look for a private place to talk. If a private area is not available, try positioning yourself in a manner that prevents others from overhearing.

Note: Public elevators and cafeterias are not considered private.

- In patient care areas such as shared patient rooms or the Emergency Department, sometimes it is difficult to prevent other people from overhearing a conversation. In these situations do your best to keep your voice to reasonable levels.
- Remember, you are to discuss PHI only with individuals who are authorized by their job to receive the information and you are to discuss the least amount of information necessary to achieve the intended business objective of the conversation.

Remember, don't snoop - don't gossip

Basic Privacy and Security Principles

Stanford HEALTH CARE

Section 3.2: Communicating with Patient Family/Friends

Discussions with patient family, friends and care-givers are confidential and should be conducted discreetly. Prior to beginning care discussions:

- Ask the patient if it is okay to have the discussion in front of his or her visitors. Be clear that you are going to discuss their medical history, their diagnosis and their treatment. Do not assume it is okay to discuss in front of visitors in the patient's room without asking.

- If circumstances do not permit you to ask the patient directly, use professional judgment to determine appropriate communications and the minimal information needed for care services.

Stanford HEALTH CARE

Section 3.3: Leaving Telephone Messages

When leaving messages for a patient, it is important to apply the following safeguards:

- Do not leave private information on answering machines or with individuals other than the patient or the patient's legal representative. You may leave a generic message using Stanford Hospital & Clinics or Stanford Children's Healthrather than the name of your department, especially in cases where the department name gives some indication as to what the patient's condition or diagnosis might be.
- Do not assume the person answering the phone is the patient's legal representative. For example, a spouse who answers the phone is most likely not the legal representative of a patient and is not automatically entitled to know PHI about his or her spouse. For minor children, follow your department's protocol for identifying the legal representative for the child.
- Each department that needs to leave messages for patients should have a protocol for doing so. Check with your supervisor regarding your department's specific protocol for leaving messages. Department or clinic managers can contact the Privacy Office if they would like their protocol for leaving messages reviewed.

Basic Privacy and Security Principles

Stanford HEALTH CARE

Section 3.4: Verification

If as part of your job function, you make calls to or receive calls from patients or others, or otherwise receive requests for PHI from people not known to you, it is important to apply privacy principles to ensure that information is provided to only those individuals who are authorized to receive information.

- If the caller or requestor is the patient or the patient's representative, obtain confirmation of the patient name and at least two other patient identifiers from the list below.

In order of priority, the acceptable verification data elements are:

- Medical record / account number
- Last four digits of social security number
- Date of birth
- Street address
- Telephone number

Note: Proper verification technique requires that when you ask for the identifier, you wait for the individual to provide you with the information. Do not offer, "you live at 234 Tree Lane, right?" or say "is your date of birth 3/20/54?

Section 3.4: Verification

Lane, right?" or say "is your date of birth 3/20/54?

Each department should have a protocol for verification procedures. Following your department's protocol, determine if the person is the patient's legal representative or someone the patient has identified as being involved in their care.

- A person listed as a patient's emergency contact or payment guarantor is not necessarily the patient's legal representative or a person involved in the patient's care and may not be entitled to receive PHI about the patient.
- If the requestor is a public official, such as law enforcement or a government agent, request to see the official's badge or other official credentials. Be sure to write down the name of the requestor, the agency the requestor works for, and the badge ID number or other credential number. Ask the requestor for a business card. If the request is in writing, the request should be on the appropriate letterhead. Be sure to ask your supervisor for assistance if you are not sure how to respond to a request for information.

If you are unsure about the verification of a caller requesting PHI, put the caller on hold and contact your supervisor or the Privacy Offices.

Basic Privacy and Security Principles

Stanford HEALTH CARE

Section 3.5: Faxing

Take frequent time-outs when sending a fax and remember the following:

- Use a fax cover sheet for every fax and indicate the total number of pages in the fax. Never include PHI on the fax cover sheet.
- If you are sending an electronic fax, confirm that the name and fax number of the intended recipient are correct.
    - Be careful of similar or same name selections.
    - Only use electronic fax solutions approved and installed by IT.

- If you are sending a manual fax, when you have finished entering the fax number, STOP: look at each digit that you entered against the actual number you intended to dial.
    - Make sure that you did not transpose numbers.
    - Pay careful attention to whether you need to dial a “9” and/or a “1” before entering the number.
    - Fax machines should be configured to print confirmation pages and generate fax transmission logs. Talk with your Supervisor if this has not already been done.

Basic Privacy and Security Principles

Stanford HEALTH CARE

Section 3.6: Copiers and Printers

You can prevent privacy mistakes from occurring by taking these simple steps when using copiers and printers:

- Immediately retrieve documents from copiers and printers
- Do not leave documents with patient information at copiers and printers unattended
- When printing from an electronic medical record or system, double-check that the selected printer location is the correct printer location for document retrieval
- When you scan a document, always clear the setting after sending the scanned document from the copier.

Section 3.7: Preventing Paper Mix-ups

Take frequent time-outs to double-check patient papers to prevent inadvertent or accidental mix-ups.

For example:

- Identify that the correct patient chart is selected before entering or printing information. Pay close attention to same name patients, and double-check to make sure that the name, date of birth, and medical record number match the intended patient.
- For same or similar name patients, guarantors, insured, or family members, take a time out, stop, and actively verify using multiple identifier checkpoints, such as date of birth or first and middle name checks, to prevent downstream billing errors with patient privacy implications.
- When mailing, faxing, or sending documents to health plans or other agencies or individuals, double-check that only documents for the intended patient are in the stack of documents to be sent or transmitted and that information about another patient is not inadvertently included.
- Before handing discharge summaries and after-visit summaries to patients, double-

Section 3.7: Preventing Paper Mix-ups

time out, stop, and actively verify using multiple identifier checkpoints, such as date of birth or first and middle name checks, to prevent downstream billing errors with patient privacy implications.

- When mailing, faxing, or sending documents to health plans or other agencies or individuals, double-check that only documents for the intended patient are in the stack of documents to be sent or transmitted and that information about another patient is not inadvertently included.

- Before handing discharge summaries and after-visit summaries to patients, double-check to make sure that the name, date of birth, and medical record numbers on the document match the patient to receive the summary.
- Double-check to make sure that addressograph labels are placed on the document for the correct patient; confirm that the name, date of birth, and medical record number match before placing the addressograph label on the paperwork.
- Whenever possible, process paperwork for one patient at a time on a clutter-free surface to prevent mistakes.

Basic Privacy and Security Principles

Stanford HEALTH CARE

Section 3.8: Keeping PHI and Work Areas Secure

Keeping your work area secure is an important part of protecting patient privacy.

Remember to:

- Keep papers and documents with patient information out of passerby's reach.
- Secure papers with patient information in locked cabinets or behind locked doors when not in use.
- Active paper records that do not need to be kept on-site may be sent to off-site storage, especially in "open plan" workspaces where lockable filing cabinets are in limited supply.
- Lock or secure workstations when walking away from your workstation or leaving exam rooms.
- Never share your passwords.

- All workstations, particularly those in public access areas, should be located or positioned so that their displays are not easily viewable by unintended parties; use privacy filters whenever possible.

Basic Privacy and Security Principles

Stanford HEALTH CARE

Section 3.8: Keeping PHI and Work Areas Secure

- Be aware of shoulder-surfing. Shoulder surfing is when an unauthorized individual attempts to see information on your computer screen by looking over your shoulder while you are working.
- Never leave workstations, laptops, USB drives (also known as flash drives or thumb drives) or other types of external hard drives that store ePHI unattended in an office (even if locked), unless the data on it is encrypted and protected with a strong password. Storage of data on such devices must be approved in writing by authorized personnel.
- Secure your physical area. Never give your security badge, card key or access code to anyone. If you are suspicious of someone in your area, ask who they are visiting and escort them to the proper location, or call Security immediately.
- Visitors, including research study sponsor staff, should not be in areas that contain PHI unless there is a business need and they are escorted by a Stanford staff member.

Section 3.8: Keeping PHI and Work Areas Secure

thumb drives) or other types of external hard drives that store ePHI unattended in an office (even if locked), unless the data on it is encrypted and protected with a strong password. Storage of data on such devices must be approved in writing by authorized personnel.

- Secure your physical area. Never give your security badge, card key or access code to anyone. If you are suspicious of someone in your area, ask who they are visiting and escort them to the proper location, or call Security immediately.

- Visitors, including research study sponsor staff, should not be in areas that contain PHI unless there is a business need and they are escorted by a Stanford staff member.

- When a staff member leaves Stanford or transfers positions, supervisors should immediately ensure that all PHI is returned to Stanford, as well as keys, badges, codes or other tools used to access PHI. Supervisors should terminate access to Stanford systems effective on the last day of employment.

DONE

Basic Privacy and Security Principles

Stanford HEALTH CARE

Section 3.9: Strong Passwords

Choosing a strong password is extremely important. Using simple, easy to guess passwords does not adequately protect patient information.

- A 14 character password is highly recommended (8 is required).
- Be sure to use difficult to guess passwords that you can easily remember. See the examples below for how to create a passphrase that is difficult to guess.
  - MCL1Z4me (My Cerner Login is for me)
  - $IZst0rd@WFB (Money is stored at Wells Fargo Bank)
  - FIar!Important2U$$ (Fidelity Investments are important to us)
  - IplaidFLUTEaz@k1d (I played flute as a kid)
- Remember, never share your password or ask someone else to share their password with you. Do not ask another person to access ePHI for you under their username.

Basic Privacy and Security Principles

Stanford HEALTH CARE

Section 3.10: Internet/Social Media

Take special care when using networking sites such as Facebook, Twitter, MySpace, blog sites, other social networks and public forums.

Remember:

- Even if you do not use a patient's name, unique circumstances involving a patient might directly or indirectly identify the patient or a patient's family members. Information that uniquely identifies a patient or a patient's family members, to include images and photographs, is protected under the law. It is against the law to use protected health information in this manner.
- Only approved personnel in Marketing and Media Relations are authorized to post photographs of patients and will ensure that patient authorization is in place for taking and posting the photo.

Basic Privacy and Security Principles

Stanford HEALTH CARE

Section 3.11: Photography

Photographs of patients are subject to privacy safeguards.

- Only authorized individuals are permitted to take pictures of patients for treatment and internal Stanford training purposes.
- Photographs taken for treatment and internal Stanford training purposes must not be used for purposes other than treatment and internal training without patient authorization or as approved by the Stanford University Institutional Review Board (IRB).
- Before photographs are taken for research or publication purposes, approval must first be obtained from the Privacy Offices.
- Special procedures must be followed for photography to occur in any other circumstance. Contact the Privacy Office for assistance. For media requests for filming, forward all inquiries to the Hospital Media Relations office or the School of Medicine Office of Communication and Public Affairs.

Basic Privacy and Security Principles

Stanford HEALTH CARE

Section 3.12: Pagers and Text Messages

Pagers and text messages are not secure communication vehicles. This means that pages and text messages can be intercepted by unauthorized individuals.

Hospital paging system:

- Only send pages with PHI when needed for critical patient care communications. You must make every attempt to use the least amount of information necessary for emergent or critical patient care delivery.

- To the extent possible, pages should be limited to alert individuals to communications that need to occur via phone or in person, or of electronic medical record messages waiting to be read.

Text messaging and Instant Messaging:

- You are not allowed to send protected health information (PHI) via text messaging or Instant Messaging. If an emergency circumstance exists where patient care and safety is at issue and there is no other means to communicate with staff, you may use this communication vehicle on a one-time, exception basis only.

Basic Privacy and Security Principles

Stanford HEALTH CARE

Section 3.13: Removable Media (Examples: External hard drives, USB drives, flash drives or thumb drives)

Stanford provides secure solutions to meet identified business needs. In most cases, secure solutions such as remote access to secure network team share drives, access to secure Web mail, or secure file transfer solutions will be able to meet your business need. Use of removable media such as USB flash drives or external hard drives for capturing confidential information, including protected health information (PHI), must not be used without approval from your supervisor and Stanford IT Security.

Supervisors may approve the use of removable media if all requirements below are met:

- The job-related business need cannot be adequately met without use of the removable media;
- You have contacted IT Security to confirm that an existing IT solution, such as VPN access, remote email access, SharePoint for team communications, Epic or Cerner communication systems or the STRIDE research system, are not able to meet the job-related need;
- The removable media has been approved by IT Security as meeting security requirements, such as encryption and password protection;
- A minimum necessary analysis has been conducted;
- A plan is in place to keep the removable media physically secure and to delete information on the removable media when the job-related task is finished.

Basic Privacy and Security Principles

Stanford HEALTH CARE

Section 3.14: Mobile Devices: Smartphones, Tablets, Laptops, and Other Computing Devices

Only staff members who have received approval from their supervisor are permitted to use mobile devices for work related purposes. Mobile devices issued by the Hospital or School are equipped with IT Security requirements. For mobile devices not issued by the Hospital or School, the following requirements apply:

- Do not use personal mobile devices to access, capture, store, or transmit patient information without approval from your supervisor and Stanford IT Security. Use of personal mobile devices without approval from your supervisor and Stanford IT Security will result in severe consequences, up to and including termination.
- Prior to the use of any personal mobile device, you must be able to verify that the following is in place:
  - Encryption (minimum 256 bit)
  - Strong password (8 characters minimum)
  - Remote data wipe software
  - Automatic timeouts are set to 10 minutes or less

Whenever possible, limit information on devices to de-identified information. If de-

Section 3.14: Mobile Devices: Smartphones, Tablets, Laptops, and Other Computing Devices

Whenever possible, limit information on devices to de-identified information. If de-identified information cannot be used, remove as many PHI elements as possible.

Delete information when no longer needed.

- For emails:
  - Do not sync work emails to your device without IT assistance.
  - Archive emails frequently to avoid large amounts of emails stored or cached on the mobile device.
- Do not share device passwords with family members, friends, or other unauthorized individual or otherwise allow access to the mobile device if it is being used to access or store ePHI.
- Keep the device in your possession and under your immediate control.
- Do not leave devices unattended in places that are not secure. A vehicle, garage, hotel room or airport is not a secure location. Protect the device in the same manner or higher as you would your personal credit card, social security card, or bank routing information.

Never capture, collect or store sensitive identifiers such as social security numbers,

Basic Privacy and Security Principles

Stanford HEALTH CARE

Section 3.14: Mobile Devices: Smartphones, Tablets, Laptops, and Other Computing Devices

Delete information when no longer needed.

- For emails:
  - Do not sync work emails to your device without IT assistance.
  - Archive emails frequently to avoid large amounts of emails stored or cached on the mobile device.
- Do not share device passwords with family members, friends, or other unauthorized individual or otherwise allow access to the mobile device if it is being used to access or store ePHI.
- Keep the device in your possession and under your immediate control.
- Do not leave devices unattended in places that are not secure. A vehicle, garage, hotel room or airport is not a secure location. Protect the device in the same manner or higher as you would your personal credit card, social security card, or bank routing information.

Never capture, collect or store sensitive identifiers such as social security numbers, credit card numbers, or other sensitive financial data on mobile devices (unless approved by the Stanford University Data Monitoring Board).

Stanford HEALTH CARE

Section 3.15: De-Identifying PHI

It is important to assume that all data requires protection under the law unless it is properly de-identified.

For example:

- When preparing slides for presentations, remember that the slides are not de-identified if any date related to a patient is present on the slide, for example, date of service or date of image.
- When using or disclosing data for analysis, remember that the data is not de-identified if city or zip code related to a patient are included in the data.
- When preparing key performance indicators or other business or clinical metrics, remember that the data is not de-identified if medical record numbers, account numbers or other numbers unique to a patient are included in the data.

Stanford HEALTH CARE

Section 3.16: Visiting Observers

SCH and SHC permit approved individuals to observe patient care and administrative functions outside of our formal training programs. Special procedures are in place and must be followed for the protection of patients and patient information.

- Visiting observer forms and training must be submitted to the Compliance Department for approval at least two weeks prior to the arrival of the visiting observer.
- Patient authorization is required when the observation is not for official SCH or SHC training programs.
- Visiting observers must have a SCH/SHC Security-issued badge and be accompanied and supervised at all times by a hospital employee, School of Medicine employee or member of the Medical Staff.
- Visiting observers must be at least eighteen years old or in a hospital-approved structured program.
- Visiting observers must adhere to all health screening requirements.

Basic Privacy and Security Principles

Stanford HEALTH CARE

Section 3.17: Contact with the Media

Special authorization requirements apply to media communications.

- For communications that involve patient information, remember to always contact the SCH News and Communications Department, the SHC Office of Communications or the School of Medicine's Office of Communication and Public Affairs before responding to any media inquiries or initiating contact with the media.
- Only individuals approved by the SCH News and Communications Department, the SHC Office of Communications or the School of Medicine's Office of Communication and Public Affairs may communicate with the media about patient information.

Basic Privacy and Security Principles

Section 3.18: Persons-of-Interest

A person of interest is anyone you might be curious about, perhaps due to the pers
status or due to an event they were involved in. The scenarios below are examples
what ***NOT*** to do. Click the **red** number to advance through the scenarios.

Basic Privacy and Security Principles

Stanford HEALTH CARE

Section 3.18: Persons-of-Interest

A person of interest is anyone you might be curious about, perhaps due to the person's status or due to an event they were involved in. The scenarios below are examples of what ***NOT*** to do. Click the **red** number to advance through the scenarios.

You see a person-of-interest, such as a celebrity, high-powered CEO, or politician, coming in for an inpatient or outpatient visit.

- You run up and introduce yourself and say what a big fan you are, or
- You talk with your co-workers about the individual and try to figure out why the individual is here for care, or
- You take a photo of the individual, or
- You tell your family members and friends that you saw this individual while at work, or
- You search for the person-of-interest's name in the electronic medical record system to see what you can find.

These are all unacceptable actions and would be subject to disciplinary action, up to and including termination.

DONE

Basic Privacy and Security Principles

Stanford HEALTH CARE

Section 3.18: Persons-of-Interest

A person of interest is anyone you might be curious about, perhaps due to the person's status or due to an event they were involved in. The scenarios below are examples of what ***NOT*** to do. Click the **red** number to advance through the scenarios.

Your coworker is in the hospital. You are concerned about your coworker so you look-up your coworker's information in the medical record to see what room she is in so that you can go and visit. You also look in the record to see when the coworker will be discharged so that you have a better idea of when she will be returning to work.

These are all unacceptable actions and would be subject to disciplinary action, up to and including termination.

DONE

Basic Privacy and Security Principles

Stanford HEALTH CARE

Section 3.18: Persons-of-Interest

A person of interest is anyone you might be curious about, perhaps due to the person's status or due to an event they were involved in. The scenarios below are examples of what ***NOT*** to do. Click the **red** number to advance through the scenarios.

A patient story authorized through the Communications Department is featured on the hospital Intranet. The story is interesting and you want to know more about the featured patient or if you or your department might have been involved in providing care or service for the patient. You look up the patient in the medical record to learn more.

These are all unacceptable actions and would be subject to disciplinary action, up to and including termination.

DONE

Basic Privacy and Security Principles

Stanford HEALTH CARE

Section 3.18: Persons-of-Interest

A person of interest is anyone you might be curious about, perhaps due to the person's status or due to an event they were involved in. The scenarios below are examples of what ***NOT*** to do. Click the **red** number to advance through the scenarios.

You hear a breaking story on the evening news about a major accident involving trauma victims being air lifted and taken to the SHC Emergency Department. When you come to work the next day, you search the medical record to see if you can find out more about the victims.

These are all unacceptable actions and would be subject to disciplinary action, up to and including termination.

DONE

Basic Privacy and Security Principles

Stanford HEALTH CARE

Section 3.19: Business Associates

A business associate does not include a health care provider involved in the treatment of a patient.

Pay careful attention when involving a business partner or associate such as a vendor or contractor in the performance of work activities that involve PHI. A business associate agreement must be in place for a person or business that creates, receives, maintains, or transmits PHI for a work-related function, activity, or service. Be sure to check with the Contracting Office to ensure a proper agreement has been executed and is on file for the vendor or contractor before allowing access to any PHI. Examples of services requiring a business associate agreement include:

- Claims processing or administration
- Data analysis
- Data processing
- Utilization review
- Quality assurance
- Patient safety activities
- Billing
- Benefit management
- Practice management
- Standard operations
- Legal
- Actuarial
- Accounting
- Consulting
- Data aggregation
- Management
- Administrative
- Accreditation
- Financial services
- Services that involve access to, use, or disclosure of PHI
- Health information exchange organizations
- Personal health record vendors
- Patient safety organizations
- E-Prescribing gateways
- Companies that facilitate data transmission

Basic Privacy and Security Principles

Stanford HEALTH CARE

Summary

In this training, you have learned about our commitment to protect patient privacy, including:

- Information that is protected under the law
- Preventing privacy breaches
- Your duty to immediately notify the SCH/SHC Privacy Office or University Privacy Office regarding potential privacy issues
- Consequences for failing to protect the privacy and security of patient information

Additionally, you have learned about basic privacy guiding principles, including:

- Principle of Minimum Necessary
- Principle of Need-to-Know
- Principle of Authorized Uses and Disclosures of Patient Information
- Principle of Verification
- Principle of Safeguarding Patient Information
- Principle of Patient Privacy Rights

Practical applications of our commitment to protect patient privacy and our privacy guiding principles were provided in this training, including:

Basic Privacy and Security Principles

Stanford HEALTH CARE

Summary

Practical applications of our commitment to protect patient privacy and our privacy guiding principles were provided in this training, including:

- Conducting confidential conversations
- Communicating with family and friends of patients
- Leaving telephone messages
- Verifying the identity and authority of persons requesting patient information
- Faxing, copying and printing patient information
- Preventing paper mix-ups
- Keeping PHI and work areas secure
- Using strong passwords and encrypting ePHI at all times
- Posting on the Internet and social media websites
- Taking photographs of patients
- Using pagers and text messaging
- Using removable media such as external drives and USB drives
- Using mobile devices such as laptops, tablets and Smartphones
- De-Identifying patient information
- Managing visiting observers
- Interacting with the media

Basic Privacy and Security Principles

Stanfo
HEALTH CA

Summary

- Conducting confidential conversations
- Communicating with family and friends of patients
- Leaving telephone messages
- Verifying the identity and authority of persons requesting patient information
- Faxing, copying and printing patient information
- Preventing paper mix-ups
- Keeping PHI and work areas secure
- Using strong passwords and encrypting ePHI at all times
- Posting on the Internet and social media websites
- Taking photographs of patients
- Using pagers and text messaging
- Using removable media such as external drives and USB drives
- Using mobile devices such as laptops, tablets and Smartphones
- De-Identifying patient information
- Managing visiting observers
- Interacting with the media
- Managing the interest in high profile patients
- Managing relationships with business associates

< P

Basic Privacy and Security Principles

Stanford HEALTH CARE

Conclusion

This training is not designed to convey every detail of complex patient privacy rules or to address every privacy issue, but it is intended to provide guidance and examples that you can use to make decisions in your daily work regarding patient privacy and security. It is important that you take time-outs in your daily routine to think about the lessons in this training before you interact with patient information. You are likely to face situations where the right course of action is unclear. The Privacy Offices and the IT Security Offices are here to provide guidance and support. The right thing to do is to call or email when you are unsure of the rules, when you have a question or concern, when there is a potential privacy violation, or just to verify your understanding of this training

SHC/SCH Privacy Office - 650-724-2572 - PrivacyOfficer@stanfordmed.org
24 hour hotline, including anonymous calls - 800-216-1784

University Privacy Office - 650-725-1828 - medprivacy@stanford.edu

Protecting Patient Privacy . . .
one patient at a time

Basic Privacy and Security Principles

Stanford HEALTH CARE

Attestation

By clicking the "I Agree" button below, I attest that I have read all of the information contained in the Protecting Patient Privacy module. I also agree to abide continuously with the organization's privacy and security policies and to report in good faith all suspected and actual violations of patient privacy to the Privacy Offices. I understand that violations of these or any other Stanford policies or regulations may be grounds for disciplinary action, up to and including termination.