

## HIPAA Communications and Office Security Guidelines

As stated in Purdue’s policy regarding Compliance with HIPAA Privacy Regulations policy VI.2.1., “Purdue University endeavors to preserve the privacy and confidentiality of the protected health information and medical records maintained by its various schools and departments. It strives to fulfill this responsibility in accordance with state and federal statutes and regulations. Further, Purdue acknowledges its general obligations of trust and confidentiality reposed in its employees and students who are responsible for medical or mental health treatment at the University. As a hybrid entity under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Purdue will ensure that its designated “covered components” comply fully with the requirements of the HIPAA Privacy and Security Regulations.

The Privacy Regulations provide that Purdue’s covered components may not use or disclose “protected health information” unless permitted by the regulations and procedures designed to protect this information. Protected health information is broadly defined and includes all “individually identifiable health information” which is transmitted electronically, maintained electronically *or maintained in any other form or medium*. In other words, the standards protect this information whether it is in paper format, computer format, or discussed orally. “Individually identifiable health information” is information which identifies or reasonably can be used to identify the individual and relates to: 1) the past, present or future physical, mental health or condition of a person; 2) the provision of health care to the individual; or 3) the past, present or future payment for the provision of health care. It therefore includes demographic information such as names, addresses, Social Security numbers, etc.

While conducting work in support of healthcare or health plan operations, we receive confidential and sensitive information in a variety of forms. This variety of communication methods creates concern about how to protect the privacy of this information while providing the quality of customer service that consumers expect. In order to assist covered entities in maintaining the privacy of individual’s health information and in order to meet our obligations as outlined in the HIPAA regulations, the following set of guidelines was formulated.

### **General Communications**

#### **Minimum Necessary:**

When using or disclosing protected health information or when requesting protected health information from another covered entity, a covered entity must make reasonable efforts to limit the use or disclosure of protected health information to the limited data set or if that is not sufficient, the minimum necessary to accomplish the intended purpose of the use, disclosure or request.

#### **Exceptions to this rule:**

- Disclosures to or requests by a health care provider for treatment
- Uses or disclosures made to the individual (e.g. patient or employee)
- Uses or disclosures made in accordance with an authorization

- Uses or disclosures that are required by law.

## **Telephone Communications and Identification of Individuals**

### **Healthcare Providers**

#### Leaving Phone Messages

When leaving a phone message for a patient to discuss treatment issues, leave your name, organization name and phone number and ask the person to return your call.

If leaving a message to confirm an appointment, it is okay to leave an appointment date and time as well as the information above, but the purpose of the visit should not be disclosed. For example, you may say, “Hello, this is the Purdue University Student Health Center. This call is to remind you of an appointment with your healthcare provider, on July 3, 2023 at 2:00 pm. If you need to reschedule the appointment, please call 494-6504, 24 hrs prior to the appointment. Thank you.”

New procedures have been developed for use of email or text messaging by health care providers or health plans in sending appointment reminders. The message must not contain PHI for this process to be used at Purdue. Please contact the Office of Legal Counsel for implementation details, (765) 496-9059.

If leaving a message regarding medical equipment that has arrived, leave a very general message stating that the person’s order is available for pick up but no details that would disclose treatment or physician identity. For example, you may say, “Hello, this is the Purdue University Student Health Center. Your order has arrived and is available for pick up in PUSH Rm B54. Please call 494-1839 if you have any questions. Thank you.”

#### Receiving Phone Calls or Identifying Individuals in Person

##### ➤ **If the individual is the patient:**

When a patient calls or appears at a clinic in person to discuss or receive *treatment or payment-related* information:

At the point of initial contact, if the patient is not well-known to personnel, confirm the identity of the **patient** by checking the following information found on a Photo ID against the medical record. If no photo ID is available or if the encounter is over the telephone, request the following information from the patient:

- ✓ Full name (first, middle initial, last name),
- ✓ PUID (if a Purdue student or employee) and
- ✓ Date of birth.

If the **patient** is not a Purdue student or employee or does not have their PUID, also verify:

- ✓ Local address.

If you are suspicious that the person is not the patient (a Purdue student or employee) they claim to be, refer to the Red Flags section below to address the situation.

During a face-to-face visit, if the patient sees additional offices within the facility and the patient is not well-known to personnel, the office staff should check the person's identity again by asking for a photo ID (if available) and verifying the following information against the medical record:

- ✓ Full name (first, middle initial, last name), and
- ✓ Date of birth.

➤ **If the caller or visitor is NOT the patient:**

If the discussion is in regards to paying a bill, you may discuss the issue with the caller or visitor only (see procedure below),

1. if you can satisfactorily identify the person, and
2. the caller or visitor is the parent of the patient who is a minor or the patient is not a minor and is covered on the caller's policy and the caller is involved in payment of the patient's account as specified by the patient either verbally or on a HIPAA authorization, (minimum necessary as pertains to the person's involvement in payment),or
3. the caller is the guarantor of the insurance policy and has received the bill (payment process only).

**Procedure**

First, **confirm the identity of the caller or visitor** by verifying their full name on a photo ID, if in person, or requesting the caller's full name, and by asking their relationship to the patient as well as how they are involved in payment for the bill. Also, ask for:

- ✓ the patient's full name,
- ✓ patient's PUID (if patient is a Purdue student or employee), and
- ✓ birth date (the patient's PUID, when available, and birth date are found on any bill from PUSH or Purdue Accounts Receivable).

If the PUID is not available or the patient is not a Purdue student or employee in addition to the above, also request the charge amount on the bill.

**To identify whether a person is involved in payment:**

1. Review notes and HIPAA authorizations in the chart or medical system (whichever is appropriate for your area) to determine whether the patient has given permission for you to discuss payment issues with a specific person or has restricted discussions with a particular person or about a particular topic.
2. Review the patient's insurance information, if applicable, to determine whether the person is the guarantor for the insurance policy.
  - ✓ If the patient is the guarantor, no information should be discussed with the caller unless the patient has provided a valid HIPAA authorization or has verbally

agreed that it is okay for the caller to discuss payment issues with the health center or clinic. A verbal okay would need to be documented in the medical system notes or chart (e.g. Patient verbally gave permission on 7/25/2006 for PUSH staff to discuss all payment-related issues with Mr. Joe Smith, patient's father and/or Mrs. June Smith, patient's mother).

- ✓ If the caller is the guarantor and provides information about the amount on the bill, only general information applying to resolution of the bill may be discussed. No treatment details can be disclosed.
- ✓ For all other callers, no information should be discussed with the caller unless the patient has provided a valid HIPAA authorization or has verbally agreed that it is okay for the caller to discuss payment issues with the health center or clinic. A verbal okay would need to be documented in the medical system notes or chart.

3. If the claim is not filed to insurance and the patient has not specifically given the caller permission to discuss payment issues either verbally or within a HIPAA authorization, no discussion about the charge can occur with the caller.

If you are suspicious that the person is not who they claim to be, refer to the Red Flags section below to address the situation.

Give only the minimum necessary information about the charge. For example, you can say that there is a charge of \$200 from PUSH on a particular date, when payment is/was due, what problem you are having with insurance. **Do not disclose treatment or diagnosis information.** If the caller wants more detailed information about the charge, see the Treatment section below.

If the call or visit is in reference to treatment, you may discuss the issue with the individual only,

- ✓ if you can satisfactorily identify the person, and
  - ✓ the caller or visitor is the parent of the patient who is a minor or they are involved in the treatment decisions of the patient as specified by the patient either verbally or on a HIPAA authorization.
- First, **confirm the identity of the caller or visitor** by verifying their full name on a photo ID, if in person, or requesting the caller's full name, and also asking their relationship to the patient. Also, ask for:
- ✓ the patient's full name,
  - ✓ patient's PUID (if patient is a Purdue student or employee) and
  - ✓ birth date.

If the PUID is not available or the patient is not a Purdue student or employee in addition to the above, also request the patient's local address.

- To identify whether a person is appropriately involved in treatment,
1. Check the age of the patient in the chart or medical system

If the patient is 18 years of age or older,

- Review notes and HIPAA authorizations in the chart or medical system to determine whether the patient has given permission or restricted discussion of treatment issues with this person.
  - If verbal or written permission has been given by the patient and no restrictions exist that prohibit you from discussing with the caller, you may discuss only the minimum necessary information for the intended purpose or what has been specified on a HIPAA authorization.
  - If no permission has been given, the caller should be informed that in accordance with HIPAA privacy regulations, the health center/clinic is only able to disclose health information to the patient or to the caller with verbal or written authorization by the patient or legal power of attorney.

If the caller is the parent and the child is under the age of 18, treatment issues may be discussed. You may discuss only the minimum necessary information for the intended purpose. Note: some issues are restricted by state law and **cannot** be discussed with the parent for children under the age of 18 (i.e. reproductive issues). Departmental policies based on state or federal law should continue to be followed.

## **Health Plan**

When individuals call to ask questions about health plan claims or benefits specific to a health plan member, first determine the relationship of the caller to the health plan member and then follow the rules below to make proper identification and determination about what information can be shared. If an employee has restricted discussions by the health plan, the restriction will be documented in a restriction folder. This folder will be maintained, and any restrictions communicated to staff by the HIPAA Privacy Liaison for the Health Plan.

- a) Employee calling about his/her own situation, confirm the following:
- ✓ Employee's name
  - ✓ Employee's PUID (if available)
  - ✓ Employee's date of birth

If the caller does not have their PUID, also ask for local address. The caller should be able to relate details regarding their health plan selections and claims.

If you are suspicious that the person is not the person they claim to be, refer to the Red Flags section below for guidance.

- b) Employee calling about his/her dependent's situation, confirm the following:
- ✓ Employee's name
  - ✓ Employee's PUID (if available)
  - ✓ Employee's date of birth
  - ✓ Dependent's name
  - ✓ Dependent's date of birth

If the caller does not have their PUID, also ask for local address. The caller should be able to relate details regarding their health plan selections and claims.

If you are suspicious that the person is not the person they claim to be, refer to the Red Flags section below for guidance.

c) Spouse calling about his/her situation, dependent's situation or calling about the employee's situation, confirm the following:

- ✓ Employee's name
- ✓ Employee's PUID (if available)
- ✓ Employee's date of birth
- ✓ Dependent's name (if applicable)
- ✓ Dependent's date of birth (if applicable)

If the caller does not have the employee's PUID, also ask for local address. The caller should be able to relate details regarding their health plan selections and claims.

If you are suspicious that the person is not the person they claim to be, refer to the Red Flags section below for guidance.

d) Friends/relatives calling on behalf of the employee, confirm the following:

- ✓ Employee's name
- ✓ Employee's PUID (if available)
- ✓ Employee's date of birth
- ✓ Name and relationship of the caller

If the caller does not have the employee's PUID, also ask for local address. If you are suspicious that the person is not the person they claim to be, require them to have the employee contact you to authorize disclosure to this person.

Be especially careful when dealing with friends/relatives who call on behalf of the employee. You need to have reasonable assurance (verbal permission or a HIPAA authorization) that the individual is calling with the permission of the employee. **If the individual does not have the specific information needed to question the situation, do not provide such information. For example, do not provide information such as diagnosis, treatment, date of service, etc. The caller should have this information, or you should refuse to answer and instead should deal directly with the employee/member.**

Only discuss specific medical and/or specific prescription drug information with the patient. Others who are involved in payment should receive only the minimum necessary information to resolve the issue. For example, if a spouse calls and wants to know why a prescription drug claim was not paid for a dependent child, over 18, and through investigation, you find that the prescription drug claim was not paid because it was for a weight loss drug, which is excluded by the plan, you should only indicate that the services provided are excluded by the plan, but do not share the actual diagnosis/procedure.

## **Business Support (i.e. Accounts Receivable)**

When an individual calls to discuss health-related charges:

Ask the caller the purpose of the call, their name and relationship to the patient.

### ► **If the caller is the patient:**

When an individual calls to discuss *payment-related* information: Confirm the identity of the caller by asking for their:

- ✓ Full name (first, middle initial, last name),
- ✓ PUID (if a Purdue student or employee) and
- ✓ Date of birth.

If the caller is not a Purdue student or employee or does not have their PUID, also ask for local address.

If you are suspicious that the person is not the patient (a Purdue student or employee) they claim to be, refer to the Red Flags section below to address the situation.

### ► **If the caller is NOT the patient:**

#### **Bill Payment**

If the call is in regards to paying a bill, you may discuss the issue with the caller only,

1. if you can satisfactorily identify the person, and
2. the caller is the parent of the patient who is a minor or they are involved in payment of the patient's account as specified by the patient either verbally or on a HIPAA authorization.

First, **confirm the identity of the caller** by asking for the caller's full name and relationship to the patient as well as how they are involved in payment for the bill. Also, ask for

- ✓ the patient's full name,
- ✓ patient's PUID (if patient is a Purdue student or employee) and
- ✓ birth date (the patient's PUID (when available) and birth date is found on any bill from PUSH or Accounts Receivable).

If the PUID is not available or the patient is not a Purdue student or employee in addition to the above, request the charge amount on the bill.

#### **To identify whether a person is involved in payment:**

If the caller is the parent of the patient who is a minor child, the bill may be discussed with the caller. Otherwise, review notes and HIPAA authorizations in the OnePurdue system or customer folders to determine whether the patient has given

permission for you to discuss payment issues with a specific person or has restricted discussions with a particular person.

If you are suspicious that the person is not who they claim to be, refer to the Red Flags section below to address the situation.

If authorized, give only the minimum necessary information about the charge. For example, you can say that there is a charge of \$200 from the clinic on a particular date, when payment is/was due. If the caller wants more detail about the charge, refer the caller to the originating department.

### **In General:**

- ✓ Be aware of your surroundings – “who can overhear?” Speak only to the intended receiver, quietly discussing confidential information.

### **Red Flags**

There may be times when you question whether you should provide information that someone requests from you. For example, a non-employee, ex-spouse calls and wants to know if his/her child is currently covered under our benefit plan. This could be a problem because the employee may not want that information shared with the ex-spouse.

If, at any time, you question the identity of the caller or whether you should be sharing information with that person on behalf of another individual, it is best to abide by one of the following instructions:

- Offer to send information in writing to the employee, patient or covered member directly;
- Offer to speak directly to the employee, patient or covered member;
- Involve your supervisor or the HIPAA Liaison;
- Instruct the person to come into the health plan or provider office with a photo ID (a Purdue ID, state issued drivers license, or state issued identification card are acceptable) to discuss the issue; or
- Refuse to provide the information.

### **Health Care Providers: Disclosures to Family, Friends, or Others -**

#### **Patient Location**

There are instances when a patient’s friend or family member contacts one of Purdue’s clinics to ask about the location of a patient or whether the patient has been seen at the clinic. Following is information provided in the Notice of Privacy Practices that addresses this issue. Also, guidance is provided to further specify the appropriate response for specific cases.

#### ***Notice of Privacy Practices***

In very limited cases, we may provide health information to family members, or close friends who are directly involved in your care or the payment for your health care, unless you tell us not to. For example, we may tell a friend who asks for you by name where you are in our



facility, and we may allow a friend or family member to pick up a prescription for you. We may also contact a family member if you have a serious injury or in other emergency circumstances. We may discuss medical information in the presence of a family member or friend if you are also present and indicate that it is okay to do so.

### *Guidance*

**Situation:** Friends or family are concerned about the whereabouts of a person. They contact the clinic to ask if a person is at the clinic or has been seen as a patient recently.

**Response:** If the patient has not been seen that day, the caller may be told that the person is not currently at the clinic. If the person has been at the clinic at any time in the past, the caller should be informed that due to HIPAA confidentiality requirements, information about patient visits is not provided. If the patient is a student, the caller can be told that in the case of a student emergency, emergency contact information, provided by the student in the University student system, is used to notify friends or family members. If the caller is still concerned about a Purdue student, they should contact the Dean of Student's office at the appropriate campus to ask for help in locating the person or contact law enforcement for help with other missing persons.

**Situation:** Purdue instructor calls the clinic to check to see whether a student was actually at the clinic and legitimately away from class.

**Response:** The instructor should be informed that due to HIPAA confidentiality requirements, patient visits cannot be verified between the clinic and instructor without a written authorization from the patient. It is standard procedure for the clinic to provide a written visit verification to the patient who can then provide to the instructor.

**Situation:** An individual comes to the clinic and tells the reception area that they have arrived to pick up a patient.

**Response:** If the patient has told clinic staff that someone is coming to pick them up, the individual should be directed to the location of the patient. If the patient has not provided information about anyone coming to pick them up, the reception area should contact the office where the patient is located and tell the patient that someone has arrived to pick them up and where to meet them.

### *Mailing of Documents*

When documents are mailed via campus mail or via external mail carrier, no classification marking should be used to indicate the contents of the envelope and the envelope should be sealed in such a way that tampering would be indicated upon receipt.

Envelopes must contain a complete address and return address, even when placed in mailboxes within the same department or building.

## **Fax:**

### **Security Controls:**

Fax devices are now divided into two varieties requiring very different security controls.

#### **1. Traditional fax**

A traditional fax is one that uses an analog phone line and isn't connected to the network. These are quite secure, other than the unattended PHI that can be left laying on them.

#### **2. Fax machines with data connections**

If files from the fax are to be stored on the server, an IPsec tunnel should be established between the fax and server to address transmission security. The shared file folder should have NTFS permissions locked down to need to know personnel, and access level auditing enabled (even if there is not an easy way to report on activity) so that all accesses can be accounted for (even if computed by hand). In addition, the fax with data functionality needs to be in a secure zone, behind a small firewall or on a highly restricted segment, no access from PAL or other more open networks.

- ✓ Like a general-purpose PC, today's copier/multifunction/fax machines (MFP) contain hard drives, memory, and a CPU. Many use mainstream operating systems such as Windows and Linux. As a result, many security best practices that apply to network devices apply to MFPs as well. Please treat them as you would a computer. Consider their physical, administrative and technical security and be aware of the data they may store on their hard drives. Please contact your IT support for destruction or wiping of the hard drive in an MFP prior to returning to a vendor, replacing, or sending to salvage.

### **Sending protected health information:**

- ✓ Use fax machines located in the most confidential area possible.
- ✓ Call ahead to alert the receiver as to when the fax will be sent and double check the fax number before you send.
- ✓ Use a cover sheet with a confidentiality notice printed on it. The confidentiality notice should state:

#### ***WARNING: CONFIDENTIALITY NOTICE***

*This cover sheet and the materials enclosed with this transmission are the private, confidential property of the sender, and the material is privileged communication intended solely for the individual indicated below. If you are not the intended recipient, you are notified that any review, disclosure, copying, distribution, or the taking of any other action relevant to the contents of this transmission are strictly prohibited. If you have received this transmission in error, please notify us immediately at (xxx) xxx-xxxx or xxxx@purdue.edu.*

- ✓ Sent in error to the wrong person? Attempt to contact the person who received it. Ask the person who received the information to either return or destroy it. If the information is to be returned, ask the person to sign the "inadvertent disclosure confidentiality agreement" and return it to you with the information. If the information will be destroyed, ask the person to sign the "inadvertent disclosure confidentiality agreement" and ask the person to fill out and return the "inadvertent disclosure Confidential

Destruction Certificate”, after the information has been destroyed. Document the unauthorized disclosure using the **“RECORD OF INADVERTENT DISCLOSURE OF PROTECTED HEALTH INFORMATION”** form and give the form to your HIPAA liaison.

### **Receiving protected health information:**

- ✓ If you are alerted that incoming confidential information is expected, retrieve the transmission promptly.
- ✓ Check the fax machines regularly throughout the day and at the end of each business day to retrieve and deliver all confidential transmissions.
- ✓ Receive misdirected information? Call the sender to report the error. Tell the sender the transmission will be destroyed. Shred it.

### **Copy Machines:**

- ✓ Remain at the copier until finished if protected health information is being copied.
- ✓ Retrieve the original and double check the area for forgotten documents.
- ✓ Press “reset” when finished to clear the copier’s memory.
- ✓ If the copier jams, stay with the machine until all the paper is removed from inside the machine.
- ✓ If forgotten documents are returned to you? Document the unauthorized disclosure using the **“RECORD OF INADVERTENT DISCLOSURE OF PROTECTED HEALTH INFORMATION”** form and give the form to your HIPAA liaison.

Please remember when transferring a copier out of your department, to have the copier hard drive wiped clean or destroyed before transfer, return to a lessor or to salvage. Please refer to the University Data Handling Guidelines for more details: <https://www.purdue.edu/securepurdue/data-handling/index.php>.

### **E-mail or Text Messaging Procedures:**

All e-mail when sent at Purdue, even an e-mail that is sent to a staff member in the same building, is transmitted over the network, through an e-mail server and is stored on that server for long periods of time. This e-mail may be available as part of the public record, by subpoena or to a potential hacker, until purged from the server some months later. Also, some staff and students forward their e-mail to servers off campus using, for example, AOL or MSN addresses where length of storage and security practices vary. Text messaging is also, not secure as it is transmitted over wireless networks which may or may not be secure.

HIPAA requires appropriate safeguards for confidential information that is transmitted electronically, typically encryption for email or text messaging. Purdue does not currently have an encryption solution that is widely available for use and Purdue policy specifically prohibits the use of email or wireless communications for restricted information, therefore, you should use the following guidelines when considering e-mail or text messaging for communications that include protected health information.

- ✓ Do NOT e-mail any protected health information to a patient.
- ✓ If you need to communicate with a patient and you wish to use e-mail or text messaging to contact them, ask the individual in the e-mail or text message to contact you by phone at a particular time. Your message should be very general and should not include confidential or evaluation/treatment- related information and should not indicate that the individual is a patient.
- ✓ Use the following confidentiality notice at the bottom of your e-mail:

***WARNING: CONFIDENTIALITY NOTICE***

The information enclosed with this transmission are the private, confidential property of the sender, and the material is privileged communication intended solely for the individual indicated. If you are not the intended recipient, you are notified that any review, disclosure, copying, distribution, or the taking of any other action relevant to the contents of this transmission are strictly prohibited. If you have received this transmission in error, please notify us immediately at (xxx) xxx-xxxx or [xxxx@purdue.edu](mailto:xxxx@purdue.edu).

**IMPORTANT: The above confidentiality notice is intended for use by Purdue's HIPAA covered components only in the transmission of confidential e-mail. The notice should not be used for other purposes.**

- If a patient sends an e-mail or text requesting confidential information, you can modify and use the following sample message to respond:

Regulations require encrypted messaging systems for confidential communications. Since Purdue e-mail/text communications are not encrypted, it is the policy of the Purdue [department name] not to use e-mail/text for sharing confidential information. We are sorry if this causes inconvenience for you in receiving information from us.

**Please call the xxxxxx office.** [Dept name] office hours can be found at: <http://www.purdue.edu/xxxx>

If you have a medical emergency, please dial 911.

- You can no longer use e-mail to direct an individual to pick up an item ordered. You can use e-mail to ask them to call your office and then notify them of the arrival of the order on the telephone. You can also notify patients that an order has arrived using a secure messaging system if available in the electronic health record. You may also leave a voicemail for them that their order has arrived.

### **Social Networking Sites:**

Social networking sites (e.g. Facebook, Instagram and Twitter) are increasingly used by staff to maintain social and professional relationships with friends and colleagues. Care should be taken in ensuring that conversations do not include topics that may breach the confidentiality of employees or patients or that may cause embarrassment to Purdue University. You should not expect that any information shared on a social media site will remain “private” regardless of your settings. As stated in University HIPAA policy and within the HIPAA confidentiality agreement

that you signed, no protected health information may be disclosed, other than for appropriate business purposes, and only using approved tools and methods.

Social networking sites are not approved, and no protected health information should ever appear on these sites. Protected health information includes any information that can be used to identify an individual and that indicates that they are a patient or health plan member at one of Purdue's covered clinics or the health plan, even if the individual's name is not mentioned. Noncompliance with HIPAA policies and procedures may result in sanctions up to and including termination.

- Therefore, staff are prohibited from posting on any social media site any content that includes protected health information and/or patient images (including patient photographs, x-ray, and other diagnostic images, as well as any photographs that may depict protected health information in the background). Even though a patient's name is not shared, other information included in the discussion may be enough to identify an individual and, therefore, violate their privacy and HIPAA laws. This prohibition applies even in cases in which you believe there is no HIPAA violation because the patient has consented, or for any other reason.
- Additionally, benefit or claims details about employees should not be shared on these sites, even for business purposes.
- Opinions about process improvement or errors in providing services should be expressed to the staff member's supervisor, not on social networking sites.
- Also prohibited is usage of social media sites to provide medical advice or medical commentary on the behalf of Purdue or to use the sites to make, recommend or increase referrals to Purdue physicians.
- Sharing on social networking sites of any confidential information pertaining to Purdue University practices or administration is prohibited.

Risks to security are also present in using these sites. Information shared among participants may not be encrypted and others outside of your workgroup, including friends or friends of friends, may have access to this information.

### **Paper Filing, Storage, removing Document from the Facility**

- ✓ Lock files containing protected health information when the office is unattended.
- ✓ Keep confidential information in your work area out of sight (in folders, face down) from passersby and visitors.
- ✓ Shred or confidentially destroy materials containing protected health information. Don't throw it in the trash!
- ✓ Information containing PHI should not be removed from the facility unless necessary for limited purposes, such as transfer to a storage facility or to a physician for treatment purposes and approved by your HIPAA Liaison. Paper documents should be stored in a


locked trunk of a car and immediately removed upon arrival at the destination. Electronically stored documents must be encrypted when stored or transmitted using the approved encryption method, <https://www.purdue.edu/securepurdue/data-handling/electronically-stored-information.php>. Documents containing PHI should **NEVER** be removed from the facility for “work at home” purposes.

### **Receipt of Misdirected Protected Health Information**

Should a covered entity send protected health information to you and it was intended for a covered component outside of your area or you are not sure where the document is intended to be delivered, you should:

- ✓ Immediately contact the Office of Legal Counsel for the entity that sent the information (contact the HIPAA liaison if the information came from another covered component at Purdue) and report the inadvertent disclosure. The entity that sent the information in error will be required to investigate and possibly report the incident.
- ✓ Do not forward the documentation to another area.
- ✓ Store the information in a locked file cabinet until the Office of Legal Counsel directs you to either shred or return it to them.
- ✓ If you cannot reach the Office of Legal Counsel in a reasonable amount of time after having left a message, shred the document.

### **Computer Security:**

- ✓ Do not let another staff member use your computer while logged in as you!
- ✓ Never share your password with anyone or leave your password where another person can view it.
- ✓ Use strong passwords. Tips for creating a strong password: <https://www.purdue.edu/securepurdue/forms-and-resources/password-tips.php>
- ✓ Don't use the same password for all your accounts
- ✓ If you have access to PHI, your password should change every 90 days, even if not prompted by the system.
- ✓ Lock your workstation when you walk away (Windows logo key  + L, or ctrl-alt-del, lock workstation)
- ✓ Screensavers must be configured to enable after 15 minutes of non-activity.
- ✓ Obligations to safeguard private information continue after termination or a move to a different position.
- ✓ Never copy files containing PHI to removable media or a mobile device (such as USB drives, an external hard drive, etc), unless appropriate encryption has been applied and unless there is a compelling business reason that outweighs the risk. For guidance on appropriate encryption solutions contact ITSP via the ITaP help desk x44000.

- ✓ Never email anything with PHI (until we have an encrypted email solution). The preferred solution is to use the secure messaging option in your area’s electronic health record system or vendor provided system, if available, or to use the FileLocker tool for transmitting files containing PHI. The instructions can be found at <https://www.itap.purdue.edu/service/catalog/security/filelocker.html>. Discuss with the University HIPAA Security Analyst for solutions where the preferred solutions are not sufficient or before new options are used.
- ✓ Devices used to store PHI must have their drives destroyed upon retirement of the device. This may include but is not limited to fax machines, all in one printers, USB drives, computer drives, laptops, computers, CDs, etc.
- ✓ Computers used to access, create, or transmit PHI should be updated with operating system patches, daily virus protection updates, and application updates.
- ✓ Laptops must be encrypted. To verify this in Windows 7, go to Start/Control Panel/System and Security/BitLocker Drive Encryption. Depending on the version of operating system, there may not be a System and Security Folder. In that case, BitLocker Drive Encryption may be directly under the Control Panel.

