

Storage:

- Only use University approved storage methods for electronic PHI. If you are unsure what services are approved please contact HIPAA Privacy Program or your local IT support group.
- Do not store PHI on unapproved cloud storage services.
- If using a storage devices such as an external drive or USB, ensure that the device is encrypted using industry standard encryption.
- Do not share or attach encryption passwords to the external storage devices.
- ALL portable devices used to store or process PHI MUST be encrypted.

Consequences:

- **Audits and/or investigations by state and federal agencies**
- **Civil monetary penalties**
 - Can be up to \$50k per violation (\$1.5M cap for violations of identical provision within one calendar year)
- **Disciplinary actions up to and including termination**
- **Lose respect of the community**
 - Privacy breaches become public knowledge
- **Reputational harm for the college, center, and University.**
 - Can result in inability to obtain future grants or other funding.




Questions or concerns?

 <https://rgw.arizona.edu/compliance/hipaa-privacy-program>

 PrivacyOffice@email.arizona.edu

 520-621-1465

 1618 E. Helen St.
PO Box 210409
Tucson, AZ 85719



Research, Discovery
& Innovation



Protecting Our Patients' Privacy



Methods for safely faxing or emailing Protected Health Information (PHI)

- **Prior to faxing protected health information:**
 - Verify the intended recipient’s fax number.
 - Verify that the correct patient’s name is on each page being faxed.
- **When faxing protected health information:**
 - Use approved department fax cover sheets.
 - Enter the fax number slowly and carefully. Avoid distractions when entering the recipient’s fax number into the fax machine.
 - Check the fax machine’s digital display to verify that the correct fax number has been entered.
- **After faxing protected health information:**
 - Call the intended recipient to verify that the information has been received.

Methods for safely transporting PHI Offsite

- Limit transportation of protected health information (PHI) to the “minimum necessary” to accomplish the authorized, intended purpose.
- To prevent breaches of confidentiality or potential damage to protected information while transporting, ensure PHI is secured in a locked box/bag.
- To avoid viewing by unauthorized persons (including passers-by), the locked bag (and/or laptop) should be transported in the trunk of the vehicle or in a location that is safe from viewing through the vehicle’s windows.
- To prevent theft of protected information, PHI must be removed from vehicles immediately upon reaching the intended destination.
- ALWAYS encrypt flash drives.

Methods for securely E-mailing and securing patient information:

- Password-protect all Word and Excel documents which contain protected health information (PHI) or individually identifiable health information (IIHI).
- ALWAYS use encryption when sending email messages containing PHI ([encrypt] or [secure] when sending from xxx@email.arizona.edu)
- Use passwords on computers (including screensavers) and mobile devices.
- Always log on/off computers.
- Log off computers when stepping away.
- Do not post PHI, or other confidential information to social networking sites or elsewhere online.

Methods for safely leaving phone messages or voicemails:

- Prevent unauthorized disclosures of protected health information (PHI) via phone messages and voice mail.
- When calling to confirm appointments or procedures, remember, “Less is better.” Abide by the “minimum necessary” rule. The safest message is one that states only the caller’s name, identifies the intended recipient, provides a call-back number, and requests a call-back.
- Avoid using text messaging to transmit/share PHI.

Definition of Protected Health Information (PHI):

Individually identifiable health information relating to the past, present or future physical or mental health or condition of an individual, provision of healthcare to an individual, or the past, present or future payment for health care provided to an individual.

Protecting Personal Identifiers:

HIPAA lists eighteen “personal identifiers” which must be protected from unauthorized access or disclosure. These identifiers may only be accessed and/or disclosed as authorized by the respective patient(s) and/or legal guardian(s), except for authorized purposes of treatment, payment, and healthcare operations (TPO). See attached HIPAA Data Reference Guide for the full list of personal identifiers and additional information.