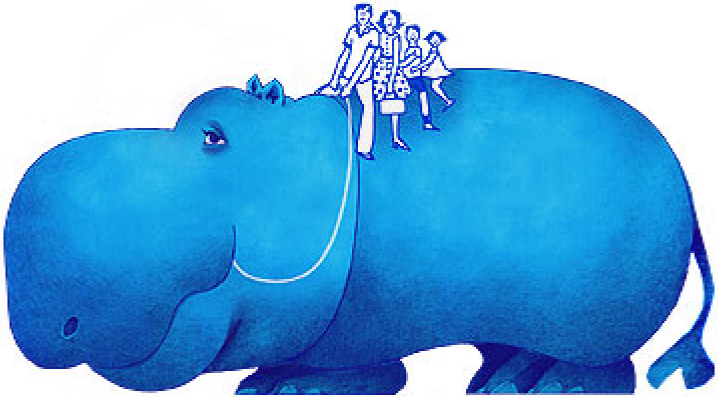
Arkansas Department of Health

Privacy and Security Training

HIPAA COMBINED SELF-STUDY MODULE



"Protecting private health information is everybody's job"

Health Insurance Portability and Accountability Act (HIPAA)

This training material is designed to help educate Arkansas Department of Health (ADH) staff members concerning HIPAA legislation, the proper use and disclosure of protected health information (PHI), the proper safeguards for confidential information including electronic protected health information (ePHI or other confidential information), and highlights from ADH HIPAA Policies and Procedures. It is not intended to replace ADH Policies. Please refer to the actual policy and departmental procedures and workflows for additional details.

HIPAA Education & Training Policy

- All members of the ADH workforce (employees, students, volunteers, business associates,) must receive HIPAA Training.
- In addition, your supervisor will provide specific training on policies and procedures in your work area.

HIPAA – What is it?

- Health Insurance Portability and Accountability of Act 1996
- Standardizes how electronic claims are processed
- Secures systems/processes that contain Protected Health Information (PHI)
- Promotes privacy/security of individually identifiable health information (IIHI)

Health information must be protected from:

- People who aren't involved in the **patient's direct treatment**
- Other employees that don't have a need to know
- Insurers using it to deny life or disability coverage
- Employers using it in hiring/firing decisions
- Reporters
- Nosy neighbors, family members, or coworkers

Key HIPAA Standards and Timelines

1. Privacy Rule – Effective date - April 14, 2003.

- Imposes restrictions on the use and disclosure of protected health information (PHI) by ADH and its employees.
- Protects individually identifiable health information that is used/disclosed in any form-electronic, paper, or oral.
- PHI is to be used or disclosed for health purposes only, with a few exceptions.
- Use/disclosure of PHI is limited to minimum necessary.

2. Electronic Transactions & Code Sets - Effective date – October 16, 2003.

- Standard electronic formats for claims and billing.
- Uniform codes that all insurance plans must use.
- Rule covers defined electronic transactions. Examples include claims, enrollment, eligibility, and payment and remittance advice.

3. Security - Compliance date - April 20, 2005 designed to ensure the security and integrity of electronically stored health information.

Definition of PHI

Protected Health Information (PHI) is any health information that may identify the patient and that relates to:

- Past, present or future physical or mental health condition
- Health care services provided
- Payment for health care.

Examples of PHI include but are not limited to:

- Patient status boards
- Eligibility printouts
- Financial records
- Fax sheets
- Test results
- Data stored on internet/intranet or portable electronic devices
- Data used for research purposes.
- A sign-in sheet that includes a patient’s name and reason for visit
- A patient's identification bracelet
- An insurance card
- A detailed appointment reminder left on an answering machine.

WHEN IS PHI NO LONGER “IDENTIFIABLE?”

Answer: When the “identifiers” about the patient (**and** the patient’s **relatives, employer and household members**) are removed.

A person’s identity can be discovered without knowing the person’s name. For example, a home address, or the name of a parent, or the name of the employer, or the children’s names could be used to determine a person’s identity, without any other information. Therefore, the HIPAA Regulations provide that – until the “identifiers” about a person are removed – any health information about that person that includes even one “identifier” is PHI and is protected by HIPAA.

There are eighteen PHI identifiers, and they apply to patients, relatives, employers or household members of the patients.

•Name	•Address (street address, city, county, zip code (more than 3 digits) or other geographic codes)
•Dates directly related to patient	•Telephone Number
•Fax Number	•email addresses
•Social Security Number	•Medical Record Number
•Health Plan Beneficiary Number	•Account Number
•Certificate/License Number	•Any vehicle or device serial number
•Web URL	•Internet Protocol (IP) Address
•Finger or voice prints	•Photographic images
•Any other unique identifying number, characteristic, or code (whether generally available in the public realm or not)	•Age greater than 89 (due to the 90 year old and over population is relatively small)

ADH Confidentiality Policy

Confidential information at ADH includes:

- Protected Health Information (PHI)
- Electronic Protected Health Information (ePHI or other confidential information)
- ADH research project information
- Confidential employee and BA information
- ADH proprietary information
- Sign-on and password codes

ADH Confidentiality Policy highlights:

- Unlawful or unauthorized access, use or disclosure of confidential information is prohibited.
- Never share or post your password
- Do not access information except to meet needs specific to your job.
- Signing the ADH Confidentiality Agreement is a condition of employment at ADH.

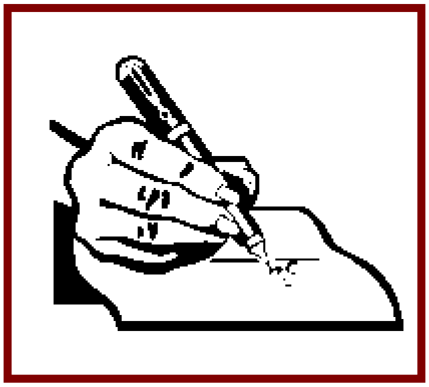
ADH Notice of Privacy Practices Policy

ADH must give our patients a copy of our "Notice of Privacy Practices" no later than the date of the first delivery of service. The Notice describes:

- How health information may be used and disclosed
- The patient’s rights
- Our organization’s responsibilities
- How to file a complaint
- Who to contact for more information

Notice of Privacy Practices

- Except in emergency situations, we must make a good faith effort to obtain written acknowledgment that our patients received the Notice.
- If unable to obtain acknowledgment, we must document why.
- The ADH Notice of Privacy Practices is posted in our buildings and on our website.
- Both English and Spanish versions are available



Scenario

Ms. Harley comes to the LPH Clinic for a pregnancy test. This is her first visit to ADH since the April 14, 2003 HIPAA Privacy compliance date. Ms. Harley is given the Notice of Privacy Practices (NPP) and is asked to sign the Acknowledgement. Ms. Harley refuses to sign the Acknowledgement. The front desk clerk tells her she cannot be seen by the RNP unless she signs the Acknowledgement. Ms. Harley leaves upset. Was the statement the clerk made to Ms. Harley **True or False?**

Answer: **False**. Treatment is not withheld because the patient refused to sign the acknowledgement. Documentation that an effort was made in good faith and that the patient refused should be noted on the acknowledgement form and included in the patient's chart.

ADH Use and Disclosure Policy

ADH policies and procedures outline how protected health information (PHI) can be used and disclosed.

- **Use** is the sharing of Protected Health Information (PHI) within the ADH community, which includes ADH off-campus facilities such as local health units

- **Disclosure** is releasing or providing access to PHI to anyone outside ADH**.**

- Generally, you may use and disclose PHI for treatment, payment and healthcare operations (TPO) of our organization WITHOUT patient authorization.

- If the requestor is not known to you, VERIFY their identity and authority before providing PHI.

Treatment Payment and Operations (TPO)

ADH can use and disclose PHI for treatment, payment and health care operations (TPO) as described in our Notice of Privacy Practices and in accordance with our policies.

- **Treatment** - Provision of healthcare by healthcare providers including coordination of care and referrals to other providers.
- **Payment** - Activities related to reimbursement and premiums such as billing, utilization review, and eligibility determinations.
- **Operations** - Examples are: training programs, accreditation, credentialing, quality improvement activities, case management, and business planning.

Note: Research is not a part of treatment, payment or operations and an employee can't copy portions of patient records that includes PHI to validate personal work performance for evaluation purposes.

Disclosures Required by Law

Limited PHI may also be used or disclosed without patient authorization when required or permitted by law. Examples are:

- Communicable disease reporting
- Suspected abuse and neglect
- Reporting to the FDA
- Organ donation purposes
- To funeral directors

Authorizations

- **Except for TPO or when required or permitted by law, most other uses and disclosures require patient authorization. Examples are disclosures to attorneys and life insurance companies.**
- The **ADH Authorization for Release of Information Form** includes the elements of a valid authorization required by HIPAA
  - Authorizations must specify data to be used/disclosed, the persons authorized to provide and receive the data, and the purpose of the use or disclosure.
  - Authorizations must include expiration date or event and be signed and dated.
  - In addition to the "core" elements above, several statements must be included regarding revocation, conditional treatment and re-disclosures.

Treatment cannot be withheld for refusal to sign Authorization unless the treatment is part of a research study and then research related treatment may be withheld.

Anyone processing or obtaining release of information/authorizations must ensure all of these elements is included when authorization is required.

No Authorization is needed for standard treatment, payment, or operations.

Scenario:

A family physician in private practice calls an ADH Local health clinic with a request for an STD consultation.

The ADH Nursing Coordinator asks for the name of the patient, the reason for the consultation request, the patient's history, and present medications.
The family physician will not provide any or all of this information for fear of violating HIPAA.

Would this in fact be a HIPAA violation?
Answer: No, the referring physician could give this information to the LHU without fear of violating HIPAA. Since the referral is for treatment purposes, no authorization is needed to release that information.

Minimum Necessary Guidelines

When using or disclosing PHI or requesting it from another organization, we must make reasonable efforts to limit it to the smallest amount needed to accomplish the task.

- If the entire chart is not required, only ask for the information you need.
- Exceptions to the Minimum Necessary include disclosures to or requests by a healthcare provider for treatment purposes

Ways ADH meets the Minimum Necessary Requirements include:

- Identifying the types of information different groups of ADH employees need to do their jobs and making reasonable efforts to limit access to only that data. That is why a clerical person has different computer privileges than a nurse does. They need different information to do their jobs.
- Requiring that employees access and share private patient information only on a "need-to-know" basis as part of their job duties. In other words, you can only view information related to the job you are doing, as outlined in the ADH Confidentiality Agreement you sign. This patient information should not be shared with others who do not have the "need-to-know" inside or outside of ADH.
- Developing policies and procedures that address the information we request from and provide to outside organizations.

Follow the simple "need to know" rule.

Sharing information with Family and Friends Involved in the Patient's Care Policy

A patient's spouse, other family member or friends may request information regarding the patient. You may share information only if you have been given permission by the patient or the patient is a minor.
Exception is for family planning. A minor receiving Family Planning services must give permission for PHI to be released to parents or guardians.

Patient Rights HIPAA gives patients the right to:

- access, inspect and copy PHI
- request amendment of PHI
- receive an accounting of disclosures
- request restrictions on disclosures
- request communications of PHI at alternative locations or means
- register complaints concerning their privacy rights.

Our contact numbers for privacy complaints are:
501- 661-2609 or 501-661-2000

When you encounter a request related to a patient right under HIPAA you should refer to the specific policy/procedure in your area that addresses it. If you still have questions, ask your supervisor. Although the patient has the right to make these requests, ADH is not always required to grant the request.

The following are some general guidelines regarding patient's rights.

Right to Access, inspect, and receive copies of PHI Policy

With a few exceptions, patients can access, inspect and receive copies of their health information.

- The request must be granted:
  Within 30 days if PHI is on-site
  Within 60 days if PHI is off-site
- If access to certain PHI is denied, then only the denied information may be withheld, and the rest of the information must be provided

ADH Amendments to PHI

Patients have a right to request an amendment if they believe their information is inaccurate or incomplete. Examples of when the amendment request may be denied are:

- When the PHI is already accurate and complete
- When the PHI was not created by the provider and the creator is available

ADH Accounting for Disclosures

A patient ***has the right*** to receive an accounting of PHI disclosures.
An accounting of disclosures includes:

- The date of each disclosure
- Who received the PHI and their address if known?
- A brief description of the PHI disclosed
- A brief statement of the purpose of the disclosure

Disclosures **exempt** from accounting include disclosures:

- For treatment, payment, or health care operations
- based on a patient's signed authorization

Examples of disclosures that must be included are those required by law such as communicable disease reporting, reporting to the Cancer Registry, and reporting to the FDA.

Scenario

A patient requests an accounting of disclosures. The LHU produces a list of the following:

1. A report to the State Health Department of a STD;
2. The provision of a copy of the patient's medical record to an attorney under a written patient authorization; and
3. An instance where progress notes were provided to the patient's PCP.

Which one of these is the one that should be included in the accounting of disclosures?

Answer: 1. a report to the State Health Department of a STD is the correct answer because it is required by law and does not require patient authorization. This disclosure must be included in an accounting of disclosures.

2. Disclosures **do not** have to be accounted for if the patient has signed an authorization for that disclosure.

3. Progress notes provided to the PCP are considered in the scope of treatment.

Disclosures for treatment, payment, and operations do not require authorization and do not have to be included in an accounting.

Privacy Rule Administrative Requirements

The Privacy Rule requires privacy policies, procedures, and systems, such as:

- implementing “safeguards”
- selecting a Privacy Officer
- providing privacy training for the workforce
- setting sanctions for violations

“Reasonable Safeguards”

ADH must take reasonable steps to make sure PHI is kept private.
Permitted (with reasonable precautions):

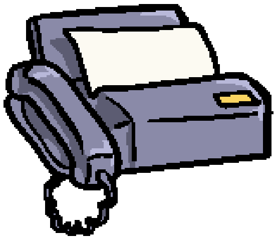
- Calling out a patient’s name in a waiting area
- Use of a sign-in sheet containing limited information.
- Talk about a patient’s care at the front desk or in hallways

ADH Safeguard Policy

- Do not leave PHI on unattended desks, computer terminals, fax machines, or copiers.
- If you happen to notice PHI that is left out, don’t read through it; close it, cover it, or put it away.
- After business hours or when not in use, PHI should be supervised or kept in a locked location.
- Avoid discussing PHI in public areas such as hallways and break rooms.
- Dispose of PHI properly by shredding or placing in a locked shredding bin.

ADH Faxing Policy

- Fax machines must be in a secure location
- Confidential data should be faxed only when mail will not suffice.
- Faxes containing PHI and other confidential information must have an official ADH fax cover sheet
- Reconfirm recipient’s fax number before transmittal
- Confirm receipt of fax
- Notify your supervisor if a fax is sent to the wrong recipient



Business Associate Policy

If ADH provides PHI to an outside entity to perform a function for or on behalf of ADH, HIPAA requires that we enter into a Business Associate Agreement that specifies how they will use and safeguard our patient information. Examples of our business associates include IHS nurses and personal care aids, and software vendors

HIPAA Research Policy

Research is **not** considered a part of "operations" and requires a consent form and HIPAA Authorization.

- HIPAA permits use of de-identified data (defined as removal of 18 specific identifiers listed above) for research purposes without authorization.
- HIPAA permits use and disclosure of a limited data set (includes some of the items removed above) provided a data use agreement is obtained.

As required by FDA and OHRP, individuals must sign informed consent to participate in a clinical trial.
• There are special rules regarding pre-research and research on the deceased.

HIPAA Security Rule – General Requirements

The HIPAA Security Rule compliance date is April 20, 2005. It requires additional protections for electronic PHI (ePHI or other confidential information).

The primary focus of the HIPAA Security Rule is to:

- Protect electronic Protected Health Information (ePHI or other confidential information) against unauthorized access, and improper alteration or destruction.
- Protect against threats or hazards to the security and integrity of ePHI or other confidential information.
- Protect against unauthorized uses or disclosures of ePHI or other confidential information.
- Make ePHI or other confidential information readily available to authorized personnel when needed.

To do this, security measures must be in place, and it is your job to abide by the ADH policies to meet the HIPAA Security requirements.

What is Electronic Protected Health Information (ePHI or other confidential information)?

Electronic Protected Health Information (ePHI or other confidential information) is PHI created, received, stored or transmitted electronically.

Examples of ePHI or other confidential information include, but are not limited to:

- Laboratory results that are emailed to a patient
- Demographic information about a patient contained in ADH information systems
- A note regarding a patient stored in your Palm Pilot, calendar on your Blackberry phone or flash drive
- billing information that is saved to a CD or disk or flash drive
- A digital photograph of a patient stored on your hard drive.

The Security Rule covers all electronic media.

- Computer networks, desktop computers, laptop computers, flash drives, personal digital assistants (PDA) and handheld computers are all considered “electronic media.”

- Electronic media also includes magnetic tapes, disks, compact disks (CDs), external hard drives, blackberry phones, and other means of storing electronic data. (This includes the Internet and ADH Intranet.)

What must ADH do?

Facility Physical Access Controls

The Security Rule lists a wide range of activities for which ADH must provide protection.

For example, we must safeguard:

- Computer hardware and software.
- Buildings that house computer hardware and software.
- Storage and disposal of data and the back-up of data.
- Who has access to data?
- Visitor access to any facilities.

There are three categories of Security "standards:"

- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards

Administrative Safeguards

- ADH must have policies and procedures in place to make sure that all members of the workforce have appropriate access to electronic PHI in order to perform their jobs.
- ADH must prevent inappropriate access.
- ADH has appointed a Security Officer. The ADH Security Officer can be reached at 501-661-2989

As an ADH Workforce Member, your role is to be familiar with and follow these policies and procedures to protect electronic patient information. You also must take steps to make certain ePHI or other confidential information is not inappropriately seen or altered.

Information Security and Password Management Policy

Password Management

Choosing a good password and keeping it secure are two of the most important steps you can take to protect electronic information.

Password Reminders

- Keep your passwords confidential. **Never share your password!**
- Avoid maintaining a paper record of passwords.
- Change passwords when there is an indication of possible compromise.
- Do not use the same passwords for business and personal accounts.
- Change passwords at regular intervals (90 days) and limit reusing old passwords on domain log-on accounts.
- Change temporary passwords at first log-on.
- Do not include passwords in any automated log-on process, including web pages.
- Always maintain and use passwords in a secure and confidential manner.
- Password phrases or sentences are encouraged for domain log-on.

Selecting a strong password

Passwords should be:

- A minimum length of six characters.
- Based on something besides personal information so that they cannot be easily guessed or obtained. For example, do not use names of family members or pets.
- composed of a mix of numeric and alphabetical characters.
- Examples of strong passwords are:
    - o #G65c1
    - o jOke51mn
    - o The sky is blue and orange! (as a domain log-on password phrase)

Security Login Monitoring Policy

Report Unauthorized Access/Use

If you believe that someone else is inappropriately using your ID or password, immediately notify the Security Officer at 501-661-2989

Disciplinary Action

You are personally responsible for the access of any information using your password. You are in violation of ADH policies and subject to disciplinary action if you access information that you do not need to perform your job at ADH or allow someone else to access information using your logon information whether they are authorized to view that information or not.

Scenario:

Janie, a new employee in your clinic, has not received her log-on to the encounter management system and scheduler. You really need help scheduling appointments. You know that Michael, the other clerk, keeps his password under his keyboard. What should you do?

A. Let Janie use your password to the appointment system.

B. Tell Janie you are sure Michael won't mind if she just "borrows" his password since he is off today. Show her where he keeps it.
C. Let your supervisor know so she can make sure she submitted a request for Janie a log-on to the appointment system. Remind Michael about the proper way to store his password.

Answer C is the correct answer. In the interim, Janie will not be able to use the appointment system since sharing of passwords is prohibited by ADH policy, and you and Michael will be held accountable for information accessed under your log-on. It is preferable not to write your password on paper. If you do need a written record, it must be kept in a secure location and should never be posted on or around your computer.

Information Access Management

Access to confidential information and ePHI or other confidential information is granted to authorized individuals on a need-to-know basis.

- ADH computers should be used only for authorized purposes. Do not access information outside the performance of your job duties.
- Do not use computers to engage in any activity that is illegal under local, state, federal, or international law.
- Do not use computers to engage in any activity that is in violation of ADH policy. For example, do not access inappropriate or offensive websites, engage in gambling, send malicious emails, or download copyrighted materials.
- Never disclose or provide **ePHI or other confidential information** to others except in accordance with ADH policies and procedures.

Scenario:

Your co-worker had a pap smear previously and it was not good. She had it redone by the RNP in the LHU. You are worried about her and are anxious to get the results. What should you do?

A. Check for lab results.
B. Call a friend who works in pathology and ask her to get the report for you.
C. Wait for your co-worker to share her pap result with you.
The correct answer is C. You should wait for your co-worker to share the results with you if she chooses to do so. You should never access patient information **outside the performance of your job duties**, and you should not ask a "friend" to do so either.
Inappropriate access to patient information can result in disciplinary action up to and including termination.

Log-on and Access Monitoring

- ADH monitors log-on attempts to the ADH electronic information systems.
- **If you suspect inappropriate log-on attempts, you must report it to IT Security**

For example, if you don't share a computer, and you notice another user signed on your computer while you were away at lunch either confirm the user has used their log-on or report appropriately.

- You must only access ADH information systems through your username and password.
- **All ADH computer systems are subject to audit and your access may be monitored**.

Information Access for Transferring and Terminating Employees Policy

- Department supervisors are responsible for reviewing transferring employees' computer access levels and notifying the department's IT administrator or the ADH IT Security Office at 501-686-6207 so appropriate adjustments can be made.
- Upon separation from ADH, all access is terminated.

Access Controls for Confidential Information

When leaving a computer unattended, log of f. Do not shut down the computer because there are automatic server updates for security.

Malicious Software

To protect against malicious software such as "worms" and "viruses":

- Anti-virus software is installed and kept current on all required information systems.
- Never bypass or disable anti-virus software.
- Email attachments are scanned for viruses prior to delivery. However, you should delete emails before opening when they appear suspicious, or if you do not know who sent the email.
- If you detect or suspect malicious software or a virus, notify the ADH Help Desk or HIPAA Security Officer immediately.
- Do not install personal software or download Internet software, such as Kazaa, anti-virus software, weather bug, and/or pop-up blockers onto ADH computers.
- Downloading Internet software onto your computer may install spy ware without your knowledge and cause your programs to run slower or not function properly.

Security Reminders

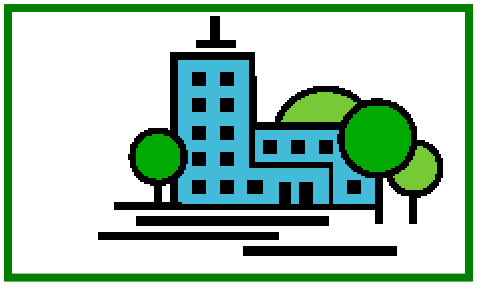
ADH provides all users with information, reminders, and updates to reinforce security training and to provide additional information. Topics include:

- ADH information security policies
- Significant ADH information security controls and processes
- Significant risks to ADH information systems and data
- Security best practices (e.g., how to choose a good password, how to report a security incident)

Be alert to reminders located on the IT web page on the ADH Intranet.

Physical Safeguards – Safeguarding PHI

Physical Safeguards are security measures to protect ADH electronic information systems hardware and related buildings and equipment. For example, exterior doors should be locked appropriately at all times or have measures in place to screen visitors as they enter.



- PCs, mobile devices, such as PDAs, Blackberry phones, flash drives, laptops, digital cameras, CDs and diskettes, or any other devices containing confidential information or ePHI or other confidential information should be secured.
- All computers, remote and on-site, including home computers that contain ePHI or other confidential

information must be protected with a secure log-on.

- All ADH electronic media that contains ePHI or other confidential information should be marked as confidential.
- Anti-virus software approved by the ADH Information Security office must be installed on all computers that may connect to the ADH network including home computers.
- ePHI or other confidential information must be destroyed before hardware or media containing ePHI or other confidential information is disposed of or made available for re-use. Deleting the files is not sufficient to remove the information, and additional measures must be taken.
- Destruction of ADH Electronic Media may be accomplished in the following ways:
    - Break diskettes or otherwise render it impossible to re-insert it into a PC drive; or
    - Punch a hole through the entire diskette; or
    - Cut CDs into pieces with standard tin-snips; or
    - Hard drives and tapes are destroyed by ADH IT Department or its designee.

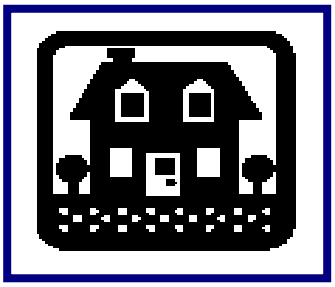
Safeguarding PHI

Working from Home

Confidentiality Extends to the Home

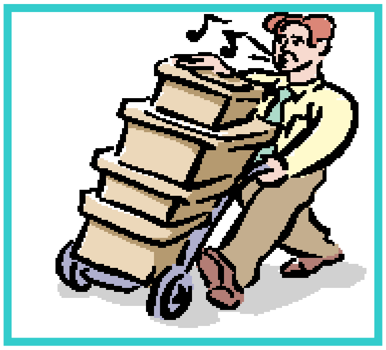
If you are assigned to work from home in an official ADH capacity, part-time or fulltime, and ADH confidential information is involved, you must sign a formal agreement outlining how information will be safeguarded

- If ADH allows you to perform some or all of your work from home, you are responsible for maintaining the privacy and security of all confidential materials.
- This includes, but is not limited to:
    - Patient Charts
    - Computers
    - Confidential Working Papers
- **All ADH confidential materials should be kept in a location that is not accessible to children, spouses, or other family members.**
- ADH materials should be put away when not being used.



Using and Transporting PHI Off-Site

Confidential information, including PHI, is not to be removed from ADH without prior approval. You are responsible for maintaining the privacy and security of all confidential information that you may be transporting, storing or accessing off-site. ADH policies are in effect whether you are off-site or in one of our facilities.



For example, if confidential information is involved:

- Any confidential information or ePHI or other confidential information sent from laptops, PDAs and other mobile devices must be encrypted and must be transported and stored in a secure manner.

One of the most common risks with these devices is theft.

- Anti-virus software must be installed on all home computers and mobile devices used for ADH business, and they must be password protected.

- Passwords must not be shared or accessible to family members or others.
- All media containing PHI must be disposed of appropriately and must never be placed in regular trash. This includes printed information, diskettes and CDs.

Removable and Portable Storage Media

Removable and portable storage media means any media that can store data digitally, can be removed from the device which utilizes the media and transported to other locations, or portable devices that have the capability to store data digitally and/or provide access to ADH systems. Examples include, but are not limited to, all non-desktop computing devices (lap tops), personal digital assistants, blackberry phones, cell phones capable of data storage, floppy disks, CDs, DVDs, USB portable drives (thumb, flash, zip, jump, pen, etc), portable music players (any mp3 player, etc.), zip disks, jaz cartridges, backup storage tapes, portable (external) hard drives, and all types of memory cards or sticks.

- Information contained on such devices can be easily compromised if the device does not have adequate protective features. These devices can be easily misplaced, lost or stolen. ***This is particularly true of USB (thumb) drives!***

- ADH data may only be stored on ADH issued media and must be encrypted.

- ADH data may not be stored on personal, non-ADH issued media.

- ***ADH employees who are issued removable and portable storage media are responsible for the security of the device and the data on the device.***

Technical Safeguards

Tracking Activity

Technical Safeguards include the use of computer technology solutions to protect electronic PHI and track activity in information systems.

Access Controls for Confidential Information

ePHI or other Confidential Information Transmissions – Encryption

When PHI or other confidential information is sent electronically from one point to another, it must be secured to avoid theft, damage, or destruction of the information.

- Encryption makes the information “unreadable” by anyone who doesn’t have the “key”.
- All transmissions of ePHI or other confidential information from ADH to an outside network must utilize an encryption mechanism between the sending and receiving entities; or the file, document, or folder containing ePHI or other confidential information must be encrypted before transmission.
- Never use an outside mail service such as Yahoo or Hotmail for transmission of messages containing ePHI or other confidential information. The ADH Exchange mail account must be used for any transmission of messages containing ePHI or other confidential information.
- When using a home computer to transmit ADH ePHI or other confidential information, use the ADH Web mail or one of the VPN services provided by ADH.

Emailing ePHI or other confidential information

Remember that ADH email resources are for official ADH business purposes only. Guidelines you should follow when emailing **PHI** include:

- Do not email patient information within the ADH Intranet and limit the information provided to the minimum necessary.
- Be careful how you ‘say things’ in e-mails and do not e-mail extremely sensitive information. E-mails are discoverable and covered by FOI act
- Do not use e-mail as your only means to communicate information that needs immediate attention. (Follow-up with a phone call or page)
- Be cautious when forwarding any emails that may contain PHI.

Domain Log-on & Email

When can I expect to get my domain logon account and email?

- 3 to 5 business days after you turn in a signed Confidentiality Agreement. Both should be ready at same time.

What will my email address be?

First name and last name separated by a period then @arkansas.gov

Example: neldia.preston@arkansas.gov

What about access to other systems that I need to do my job?

Access to additional ADH information systems is granted at the request of your supervisor after you complete any required training for that system.

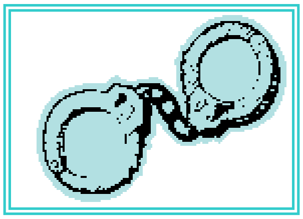
HIPAA Penalties for Noncompliance

ADH Disciplinary Notice

Employee Sanctions: Violations by ADH workforce may result in disciplinary action, up to and including termination from employment with ADH.

U. S. Government Sanctions

Severe civil and criminal penalties: In addition, you can be subject to civil and criminal penalties imposed by the federal government up to $250,000 and 10 years in prison.



Conclusion

- We must all remember to protect the privacy and security of patient information at all times.
- We are all patients ourselves from time to time. Think about how you would feel if your own health information were used or disclosed in a way that was harmful to you or your family.
- If you have a question about HIPAA, ask your supervisor or manager, or contact your ADH Privacy or Security Officers.

HIPAA Websites:

ADH HIPAA (policies and other HIPAA information)

http://healthycolleagu/HIPAA.htm

Department of Health and Human Services

http://www.hhs.gov/ocr/hipaa/finalmaster.html

http://www.dhhs.gov/ocr/hipaa/

American Medical Association

www.ama-assn.org

HIPAA Advisory

www.hipaadvisory.com

HIPAA HINTS

1. Use private areas to discuss patient information, if possible.

2. Keep the volume of your voice lowered when having conversations concerning patients in non-private areas.

3. When papers containing patient information are no longer needed or required, either shred them or place in a secure shredding bin.

4. **Before talking with a patient's family members or friends** about a patient's condition, check with the patient *first*, **or** in the patient's absence, information limited to the family member/friend's involvement in the patient's care may be shared if you can infer from the circumstances that the patient does not object, such as when the family member/friend has been present with the patient on recent visits and patient has agreed, or not objected to, their presence during your conversations with the patient.

5. **Before releasing patient information by phone**, verify caller's identity – even if it is the patient calling. If it is not the patient, then you must verify that person's identity *and authority* to have the information, or ask that the patient call instead. For example, the family member/friend situation may apply as discussed above in 4.

6. If you do not need patient information to do your job, do not seek it out. Only Access or use patient information when needed *to perform your job*.

7. Log off your computer or "lock" your workstation using Ctrl/Alt/Del when you will be away from your work area, so PHI cannot be viewed or accessed in your absence.

8. Do not share your password with anyone.

9. Be careful not to leave patient information at copy machines, fax machines, printers. In Home Services, Home Health, Hospice, Personal Care, MIP rooms staff are to protect information when transporting.

10. When faxing information, use an "official" ADH coversheet and confirm recipient's fax number and receipt of fax.

11. Medical records should not be taken off the premises. In Home Services policies will be followed to protect PHI.

12. Use privacy screens on computer monitors, or if one is not available, turn monitor so that it cannot be viewed by unauthorized persons passing by.

13. If you overhear a conversation concerning a patient, keep it to yourself.

15. Do not leave messages concerning a patient's condition or test results on any answering machine.

16. Report suspected privacy violations to the HIPAA Compliance Office by calling **501-661-2609.**

17. Patient information or chart is never to be copied and used by employees to demonstrate performance.

HIPAA PRIVACY and SECURITY TRAINING ACKNOWLEDGMENT
This is to acknowledge that I have completed the required ADH HIPAA Privacy and Security Awareness Training. Print this out for your file.

Complete the Review and Training Acknowledgement (Post Assessment) on A-TRAIN.
Instructions for taking the post assessment are provided below.

Last Name, ___________________First Name, ________________DATE,________

Employee #________________ SIGNATURE: ____________________________

Instructions for Completing the ADH HIPAA Privacy and Security Training Post Assessment on A-TRAIN

After reviewing the self-study module, learners need to **return to A-TRAIN and log in.** In "**My learning Record**, " click on **"My Learning"**. Click on the **M** next to the name of the course you just completed (ADH HIPAA Privacy and Security Training). Scroll down and click on the **completed button**. You will then be asked if you want to mark the course complete. Click **yes**. You will then be instructed that an assessment needs to be completed before you can continue. Click on the **assessment link** and complete the assessment. **(See Important Note below.)**

Important Note: The post-assessment will be displayed in a separate window. If your computer has pop up blocker enabled, this will prevent the post-assessment from being displayed. A pop up blocker can be avoided if you press the CTRL key at the same time you click on the links to open the post-assessment. This will normally allow the window to load.

If you pass the post assessment, your Certificate of Completion will be available in your A-TRAIN learning record under Certificates. Click on the course title to print a copy for your files. The certificate will remain in your A-TRAIN record.

If you fail the post assessment, you will need to re-register to take the assessment again.