Security Training

UAMS HIPAA
SELF-STUDY
MODULE

“Confidentiality is everyone’s job, not everyone’s business”

January 3, 2005
The Security Rule - Health Insurance Portability and Accountability Act (HIPAA)

This training material is designed to educate staff members concerning the Security Rule portion of the HIPAA regulations, the proper safeguards for confidential information including electronic protected health information (ePHI), and highlights from UAMS Security Policies and Procedures. It is not intended to replace UAMS Policies. Please refer to the actual policy and departmental procedures for additional details.

HIPAA Education & Training Policy # 3.1.30

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

HIPAA Security Rule – General Requirements

You have heard about the HIPAA Privacy Rule. The HIPAA Privacy Rule covered Protected Health Information (PHI) in all forms – verbal, written, and electronic. The compliance date for the Privacy Rule was April 14, 2003.

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

The primary focus of the HIPAA Security Rule is to:

- Protect electronic Protected Health Information (ePHI) against unauthorized access, and improper alteration or destruction.
- Protect against threats or hazards to the security and integrity of ePHI.
- Protect against unauthorized uses or disclosures of ePHI.
- Make ePHI 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 UAMS policies to meet the HIPAA Security requirements.

What is Electronic Protected Health Information (ePHI)?

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; or
- health care services provided; or
- payment for health care.
**Electronic Protected Health Information (ePHI)** is PHI created, received, stored or transmitted electronically.

**Examples of ePHI include, but are not limited to:**
- laboratory results that are emailed to a patient,
- demographic information about a patient contained in UAMS information systems such as eChart, WebChart and Logician,
- a note regarding a patient stored in your Palm Pilot,
- billing information that is saved to a CD or disk, and
- a digital photograph of a patient stored on your hard drive.

**The Security Rule covers all electronic media.**
- Computer networks, desktop computers, laptop computers, personal digital assistants (PDA) and handheld computers are all considered “electronic media.”
- Electronic media also includes magnetic tapes, disks, compact disks (CDs) and other means of storing electronic data. (This includes the Internet and UAMS Intranet.)
WHEN IS PHI NO LONGER “IDENTIFIABLE?” – Policy # 3.1.31

**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.

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

The Security Rule lists a wide range of activities for which UAMS 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**

- UAMS 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.
- UAMS must prevent inappropriate access.
- UAMS has appointed a Security Officer. The UAMS Security Officer can be reached at 501-603-1336.

As a UAMS 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 is not inappropriately seen or altered.

**UAMS Confidentiality Policy # 3.1.15**

**Confidential information at UAMS includes:**

- Protected Health Information (PHI)
- Electronic Protected Health Information (ePHI)
- UAMS research project information
- Confidential employee and student information
- UAMS proprietary information
- Sign-on and password codes

**UAMS Confidentiality Policy Highlights:**

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

**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:
  - #G65c1
  - jOke51mn
  - The sky is blue and orange! (as a domain log-on password phrase)

Never share passwords with others.

**Report Unauthorized Access/Use**

If you believe that someone else is inappropriately using your ID or password, immediately notify the Technical Support Center at 501-686-8555 or the Security Office at 501-686-6207. If you are an UAMS employee located at ACH or work off-campus for the Department of Pediatrics you can call TechSource at 501-364-5299.

**Disciplinary Action**

You are personally responsible for the access of any information using your password. You are in violation of UAMS policies and subject to disciplinary action if you access information that you do not need to perform your job at UAMS or allow someone else to access information if they are not authorized.
Janie, a new employee in your clinic, has not received her log-on to the appointment system. You really need help scheduling appointments. You know that Michael, the other scheduler, 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 and has scheduled her for appointment system training. 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 UAMS 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.

Computer Access

• Access to confidential information and ePHI is granted to authorized individuals on a need-to-know basis.
• UAMS 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 UAMS 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 to others except in accordance with UAMS policies and procedures.

Your co-worker had a biopsy performed at UAMS. You are worried about her and are anxious to get the results. What should you do?

A. Check WebChart for the 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 biopsy 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

- UAMS monitors log-on attempts to the UAMS electronic information systems.
- If you suspect inappropriate log-on attempts, you must report it to the IT Security Office at 501-686-6207 or the Technical Support Center at 501-686-8555 or at ACH call TechSource at 501-364-5299. 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 had their own log-on or report appropriately.
- You must only access UAMS information systems through your username and password.
- All UAMS computer systems are subject to audit and your access may be monitored.

System Access for Transferring and Terminating Members of the Workforce

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

Locking the Computer

When leaving a computer unattended, lock the computer using “control/alt/delete” or log-off the computer.

To lock the computer:
1. Press CTRL, ALT, Delete keys on the keyboard to lock the computer.
2. On the pop up window, click on the Lock Computer button.

When you want to work on the computer again, you will need to login with your domain password.
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 UAMS Technical Support Center at 501-686-8555 or at ACH call TechSource 501-364-5299 immediately.
- Do not install personal software or download Internet software, such as Kazaa, Weatherbug, anti-virus software, and/or pop-up blockers onto UAMS computers.
- Downloading Internet software onto your computer may install spyware without your knowledge and cause your programs to run slower or not function properly.

Security Reminders

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

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

Reminders are sent via email from UAMS “Mail Administration”. Be alert to reminders and follow directions accordingly.

Physical Safeguards – Safeguarding PHI Policy # 3.1.38

Physical Safeguards are security measures to protect UAMS 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, Blackberrys, laptops, digital cameras, CDs and diskettes, or any other devices containing confidential information or ePHI should be secured.
- All computers, remote and on-site, including home computers that contain ePHI must be protected with a secure log-on.
• All UAMS electronic media that contains ePHI should be marked as confidential.
• Anti-virus software approved by the UAMS Information Security office must be installed on all computers that may connect to the UAMS network. This includes your home computer.
• ePHI must be destroyed before hardware or media containing ePHI 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. Contact the Technical Support Center for information regarding this at 501-686-8555 or at ACH TechSource at 501-364-5299.
• Destruction of UAMS 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
  – Request destruction of CDs and diskettes by a shredding company contracted with UAMS to destroy diskettes and CDs.
  – Hard drives and tapes are destroyed by UAMS IT Department or its designee.

Confidentiality Extends to the Home
• If UAMS 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 not limited to:
  – Patient Charts
  – Computers
  – Confidential Working Papers
• All UAMS confidential materials should be kept in a location that is not accessible to children, spouses, or other family members.
• UAMS materials should be put away when not being used.

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

Contact the UAMS HIPAA Office, 501-603-1379, for agreement content specifications.
Using and Transporting PHI Off-Site

Confidential information, including PHI, is not to be removed from UAMS 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. UAMS 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 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 UAMS 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. (Refer to Safeguarding PHI Policy #3.1.38)

Technical Safeguards

Tracking Activity.

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

ePHI Transmission – Encryption

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

- All transmissions of ePHI from UAMS to an outside network must utilize an encryption mechanism between the sending and receiving entities; or the file, document, or folder containing ePHI must be encrypted before transmission.
- Encryption makes the information “unreadable” by anyone who doesn’t have the “key”.
- SSH, SSL or VPN secure technologies must be used for any inbound or outbound transmissions of ePHI. Call the Technical Support Center at 501-686-8555 for assistance with encryption mechanisms and keycodes.
- Email within the UAMS Intranet is automatically encrypted.
- Email sent outside of UAMS will be encrypted at the gateway if it contains ePHI. The UAMS Exchange mail account must be used for any transmission of messages containing ePHI. Never use an outside mail service for transmission of messages containing ePHI.
Emailing ePHI Policy # 7.1.12

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

- When possible, only email patient information within the UAMS Intranet.
- Limit the information provided to the minimum necessary. (Refer to UAMS Minimum Necessary Policy #3.1.25.
- Be cautious when forwarding any emails that may contain PHI.
- If you email PHI outside of the UAMS intranet, you must abide by the UAMS Email Policy #7.1.12.

Domain Log-on & Email

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

- 3 to 5 days after you turn in a signed Confidentiality Agreement. Both should be ready at same time.
- Your domain name is lastnamefirstnameinitial.
- Your initial password is your social security number, and it must be changed at first login. You must make this change from a computer on the campus network. It cannot be changed through the Internet.

What will my email address be?

- 1st Initial 2nd Initial Last name. absmith@uams.edu
- 1st Initial Last name (if you don’t have a middle initial). pduncan@uams.edu

What about access to other systems that I need to do my job?
Access to additional UAMS information systems is granted at the request of your supervisor after you complete any required training for that system. Examples may include our patient records systems, such as EPF, eChart, Logician, and appointment and billing systems such as HBOC and SMS.
UAMS Technical Support Center

The UAMS Technical Support Center (formerly known as the “Help Desk”) is available 24 hours a day, 7 days a week to assist you with computer/software related questions and problems. You can reach the Technical Support Center by:

- calling 501-686-8555 or
- emailing them at techsupport@uams.edu (Tech Support Center in the UAMS Address Book) or
- going to their website at http://techsupport.uams.edu/

You should have the following information available when you contact them:

- Last Name, First name, Domain login name
- Campus location with Room #
- Contact Phone # or Pager
- Problem description
- Application &/or Operating system name, for example: Word2003, eChart, Windows 2000 or XP
- UAMS property Tag# & computer name

ACH TechSource

UAMS employees located at ACH or working for the Department of Pediatrics off-campus should call TechSource at 501-364-5299.

ACH TechSource is available 24 hours a day, 7 days a week to assist you with computer/software related questions and problems. You can reach them by:

- calling 501-364-5299 or
- emailing them at techsource@uams.edu

You should have the following information available when you contact them:

- Last Name, First name, Domain login name
- Campus location with Room #
- Contact Phone # or Pager
- Problem description
- Application &/or Operating system name, for example: Word2003, eChart, Windows 2000 or XP
- UAMS property Tag# & computer name
UAMS Reporting Policy # 3.1.23

- All known or suspected violations of the HIPAA regulations must be reported.
- There will be no retaliation for reporting of suspected violations.
- Reports by **members of the workforce** can be made to:
  - Reporting line at 1-888-511-3639
  - HIPAA Office 501-614-2187
  - IT Security Office 501-686-6207
  - Anyone in a position of responsibility - The person receiving the report should then contact the HIPAA Office.
- **Patients and others** can use the general complaint process or contact the UAMS HIPAA Office directly.
- It is important that suspected violations be reported, so we can attempt to mitigate any harmful effects and prevent the problem from happening again.

**HIPAA Penalties for Noncompliance**

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

**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 UAMS Privacy or Security Officers.

**HIPAA Websites:**

**UAMS HIPAA (policies and other HIPAA information)**
http://hipaa.uams.edu

Department of Health and Human Services
http://www.dhhs.gov/ocr/hipaa/

American Medical Association
www.ama-assn.org

HIPAA Advisory
www.hipaadvisory.com
HIPAA HINTS

“Confidentiality Is Everyone’s Job, Not Everyone’s Business”

1. Do not discuss patient information in cafeteria lines, in elevators, or in places where persons can hear you.
2. Keep the volume of your voice lowered when having conversations concerning patients in non-private areas.
3. Place papers containing confidential information in a shredding bin or other secure container – NOT the trash can.
4. PDA’s, laptops and other computer devices should be secured when not in use.
5. Destroy CD’s and other electronic storage media containing confidential information before placing in trash containers.
6. Before talking with family members or friends about a patient’s condition, check with the patient.
7. When releasing patient information by phone, verify caller’s identity. Verify caller’s authority to receive information, if the caller is not the patient.
8. Access patient information only when needed to perform your job.
9. Log off or lock your computer when you will be away from your work area.
10. UAMS computers may not be used for activity that is illegal under local, state, federal or international law, or in violation of UAMS policy.
11. Access to UAMS computers and electronic information is audited, and employees should not have an expectation of privacy during such use.
12. Never bypass or disable anti-virus software on devices that access UAMS servers.
13. Do not share your password with anyone.
14. Where possible, close and lock doors that allow access to ePHI and/or computer resources.
15. Medical records should not be taken off the UAMS campus.
16. If you overhear a conversation concerning a patient, keep it to yourself.
17. Do not leave messages concerning a patient’s condition or test results on any answering machine.
18. Report suspected violations to the HIPAA Compliance Officer by calling 501 614-2187.

http://hipaa.uams.edu
UAMS CONFIDENTIALITY POLICY

Confidential Information includes information concerning UAMS research projects, confidential employee information, information concerning the
UAMS research programs, proprietary information of UAMS, and sign-on and password codes for access to UAMS computer systems. Confidential
information shall include Protected Health Information.

Protected Health Information (PHI) means information that is part of an individual’s health information that identifies the individual or there is a
reasonable basis to believe the information could be used to identify the individual, including demographic information, and that (i) relates to the past,
present or future physical or mental health or condition of the individual; (ii) relates to the provision of health care services to the individual; or (iii) relates
to the past, present, or future payment for the provision of health care services to an individual. This includes PHI which is recorded or transmitted in any
form or medium (verbally, in writing, or electronically), PHI excludes health information maintained in educational records covered by the federal Family
Educational Rights Privacy Act and health information about UAMS employees maintained by UAMS in its role as an employer.

POLICY: UAMS prohibits the unlawful or unauthorized access, use or disclosure of confidential and proprietary information obtained
during the course of employment or other relationship with UAMS. As a condition of employment, continued employment or relationship
with UAMS, UAMS workforce shall be required to sign the UAMS Confidentiality Agreement approved by the UAMS Office of General
Counsel. UAMS will provide training for each of its workforce members on the importance of maintaining confidentiality and the specific
requirements of state and federal law, including the HIPAA Privacy Regulations and laws protecting the privacy of students and
employees. This policy applies to information maintained or transmitted in any form, including verbally, in writing, or in any electronic
form.

PROCEDURES:

1. Confidentiality Agreement: As a condition of employment, continued employment, or a relationship with UAMS, UAMS will
require such individuals to sign the UAMS Confidentiality Agreement approved by the UAMS Office of General Counsel. The
Confidentiality Agreement shall include an agreement that the signing party will abide by the UAMS policies and procedures and
with federal and state laws, governing the confidentiality and privacy of information.

   All new employees, students, or vendors requiring access to electronic Confidential Information (computer systems) must have a
current Confidentiality Agreement on file in the IT Security Office. The UAMS IT Security Office will maintain signed
Confidentiality Agreements and furnish a copy to the individual signing the agreement. It is the responsibility of the manager
hiring individual vendors or consultants or receiving sales representatives or service technicians (who do not require electronic
access but who may have access to Confidential Information) to require execution of the appropriate confidentiality agreements
approved by the UAMS Office of General Counsel and to send those documents to the UAMS IT Security Office.

2. Restriction on Access, Use and Disclosure of Confidential Information: UAMS limits and restricts access to Confidential
Information and computer systems containing Confidential Information based upon the specific duties and functions of the
individual seeking or requiring access. UAMS will further limit and control access to its computer systems with the use of
sign-on and password codes issued by the IT Security Office to the individual user authorized to have such access.

   Authorization to access, use or disclose Protected Health Information also is governed by the UAMS Use and Disclosure Policy.

   UAMS will control and monitor access to Confidential Information through management oversight, identification and
authentication procedures, and internal audits. UAMS managers and heads of departments will have the responsibility of
educating their respective staff members about this Policy and the restrictions on the access, use and disclosure of Confidential
Information, and will monitor compliance with this Policy.

3. Sales Representatives and Service Technicians: Must register in the appropriate area (Refer to UAMS Guidelines for Vendors
and Sales Representatives Policy), sign and complete the Confidentiality Agreement prior to any exposure to UAMS
Confidential Information.

4. Media: All contacts from the media regarding any Confidential Information must be referred to the UAMS Office of
Communications and Marketing (501-686-8998 or pager 501-395-5989)

5. Violation of Confidentiality Policy: Individuals shall not access, use, or disclose Confidential Information in violation of the law
or contrary to UAMS policies. Each individual allowed by UAMS to have access to Confidential Information must maintain and
protect against the unauthorized access, use or disclosure of Confidential Information. Any access, use or disclosure of
Confidential Information in any form – verbal, written, or electronic – which is inconsistent with or in violation of this Policy
may result in disciplinary action, including but not limited to, immediate termination of employment, dismissal from an academic
program, loss of privileges, or termination of relationship with UAMS.

   All UAMS employees and others subject to this Policy must report any known or suspected incidents of access, use or disclosure
   of Confidential Information in violation of this Policy or in violation of the law.
1. Logging onto the Network and allowing someone else to use the computer is against UAMS Policy.
   A. True
   B. False

2. Which is the best way to protect sensitive data in your computer when you go out for lunch or home for the evening?
   A. Turn your monitor off
   B. Activate the screen saver
   C. Lock your computer
   D. Close all programs

3. Identify examples of computer safety:
   A. Create alpha numeric passwords
   B. Locking computer screens while away
   C. Log off computer at the end of workday
   D. All of the above

4. Which of the following are strong passwords?
   A. Steve
   B. My dog’s name
   C. #G6cZ
   D. My last name spelled backwards
   E. *j 0ke5lmn

5. Other than yourself, who else should know your password?
   A. Only your supervisor, major professor, or system administrator
   B. Coworker
   C. No one

6. When a computer virus is detected or suspected it must be reported to the UAMS Information Security Office within what time frame?
   A. Immediately
   B. Never
   C. Within 24 hours

7. Of the following choices, which indicates when it is safe to open a file attached to email?
   A. When you know the sender, the attachment is expected, and it is not unusual in anyway
   B. When the email is only sent to you
   C. When you know the sender

8. Are you free to do whatever you want with your network-connected computer?
   A. Yes. It is my personal computer and I can do what I please.
   B. No. I have to be a responsible member of the networked community and am bound by UAMS policy.
9. **Downloading internet files, such as screensavers, Kazaa or Weatherbug may install spyware onto my computer without my knowledge and cause my programs to run slower or not function properly.**
   A. True
   B. False

10. **If someone gains access to my passwords, what are some of the possible repercussions?**
    A. I may have files deleted from my computer
    B. ePHI may be viewed/used in violation of HIPAA
    C. My Computer may be used to commit a crime
    D. All of the above
HIPAA SECURITY TRAINING ACKNOWLEDGMENT

This is to acknowledge that I have completed the Required UAMS HIPAA Security Awareness Training.

Complete the Security Review and Training Acknowledgement.

Send to UAMS HIPAA OFFICE, # 829