Release of Information and Breach Prevention and Reporting Highlights for CUMG

Presented by the

UAMS HIPAA Office

March 15, 2016

Why HIPAA Matters

- HIPAA is the law, but in the end protecting patient confidentiality is how we show we care.
- 99.2% of our patients - “It is important to me that members of my health team respect my privacy when I am at the hospital or clinic”

Identifiers that are PHI (Protected Health Information) – here's what we need to protect!

Apply to patients, their families, household members and employers:

- Name
- Address (street address, city, county, zip code (more than 3 digits) or other geographic codes)
- *Dates related to patient*
- Age greater than 89
- Telephone Number
- Fax Number
- E-mail addresses
- Social Security Number
- Medical Record Number
- Health Plan Beneficiary #
- 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)*

For every request for information, ask yourself

- Who am I speaking with?
- Who is requesting the information?
- What is his/her authority to have the information?
- Who is the patient ?
- What information is being requested?
- What is the purpose of the request?
- Are there any restrictions in place regarding release of this patient's information?

Disclosing PHI

- If the requestor is not known to you, always **VERIFY** their identity and AUTHORITY before providing **PHI**.
- Have the person provide the information rather than just confirming the information.
- For example, ask them for the patient's address rather than saying " Do you still live on XYZ Avenue? "

Verifying identity of patient

Obtain any 3 of the following patient items:

- Full name
- Date of Birth
- Last 4 digits of SS number
- One additional piece of information such as address, phone, acct number

Verify Identity of Requestor if not known to you

- Caller's name
- Company name/relationship to patient
- Phone number
- When in doubt, call the phone number for the entity requesting the information or have them fax a written request on company letterhead

Then verify authority to have the information

When the patient is the requestor Patient's Right to PHI

- With a few exceptions, patients or their legal representatives, have a right to copies of their medical record, including billing records, within 30 days of requesting them.
- Patients have a right to electronic copies of their records.

Real Life Example

- A clinic failed to provide 41 patients with copies of their medical records when they requested them.
- When the OCR investigated, the clinic did not adequately respond to the investigation.
- They were was fined $4.3 Million.

Use and Disclosure 2.1.13

- Generally, you may use and disclose **PHI** for treatment, payment and healthcare operations (TPO) of our organization **WITHOUT** patient authorization.
- Most of your uses (within UAMS) and disclosures (outside UAMS) of PHI for TPO, will be for Payment purposes.

Patient Authorization

- HIPAA generally requires that a patient sign an Authorization for disclosures (sharing protected health information – PHI – with someone outside of UAMS) made for purposes other than TPO
- Use your Authorization check list to make sure the Authorization is valid.
- Make sure the authorization has not expired and is signed by the patient or the patient's documented legal representative.
- Verify signatures against documents on file
- There are certain exceptions to this rule, such as when the disclosure is required or permitted by law, and an authorization is not required in those cases.

An Example of When an Authorization Is Not Required

- Subpoenas for Parties in Litigation – One of the following is required:
  - Patient authorization, or
  - Court order, or
  - Adequate assurances that the party whose PHI is requested has been given notice of the request with adequate time to object, and that no objection was made

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

You may share information **directly relevant** to the person's involvement with the patient's care or for payment related to care under the following circumstances:

If the patient is present or otherwise available prior to the disclosure, you must:

- Obtain the patient's agreement **or**
- Provide the patient an opportunity to object, and they do not **or**
- Using professional judgment, reasonably infer from the circumstances that patient does not object.

MCPG Procedure for speaking with a patient's family member or friend

If written Authorization for ROI is not on file:

- Obtain verbal permission and document in comments that patient was identified and gave verbal permission.
- Send an Authorization for ROI to patient.
- Document your actions and follow procedure for processing the Authorization when it is returned.

If the patient is not available or is incapacitated

- If there appear to be extenuating circumstances, for example the patient is incapacitated and doesn't have a legal representative to act on their behalf, you should get your supervisor involved.
- If the family or friend wants to make a payment and is just asking for the balance, verify in notes that the person has been making payments. If so, you may provide the balance

Patient Rights
Restriction Requests 2.1.19

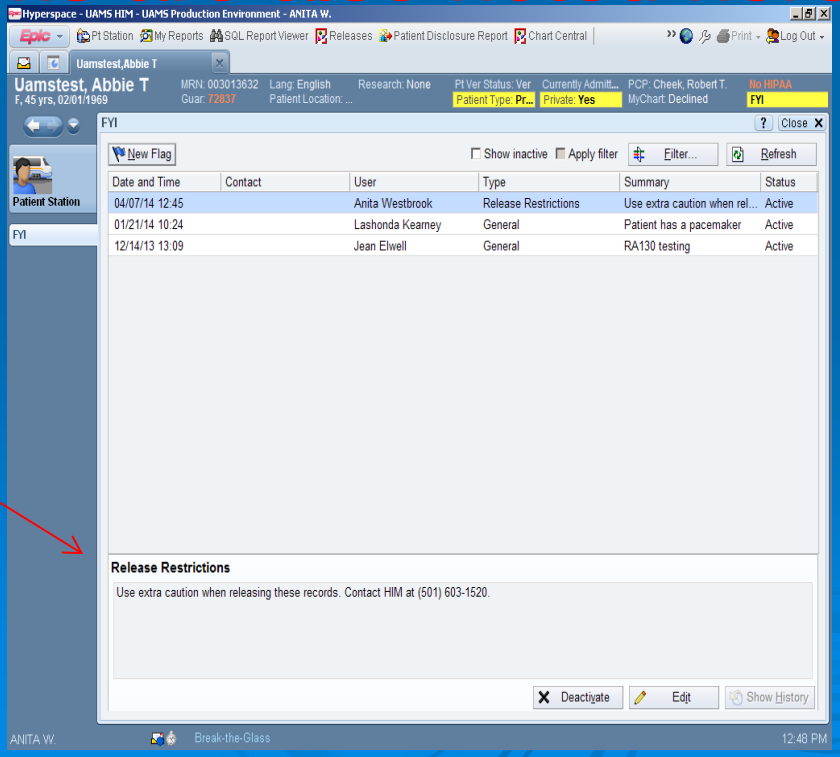
- Have patient fill out ***Patient Request to Restrict Use/Disclosure*** **Form** (Med Rec 2348) or refer them to the HIPAA Office.
- All Restriction requests must be sent to UAMS HIPAA Office for processing.
- The HIPAA Office, in conjunction with HIM and other departments affected by the request, will determine whether it will be agreed to or denied.
- Follow your procedure for making staff aware of any restriction we agree to. Always check FYI flags before releasing patient information.

Restriction Requests

While UAMS is evaluating a Restriction Request, you might see a Release Restrictions FYI Flag. Click on the flag and follow the instructions associated with that flag. Revocations of Authorizations are also noted here.

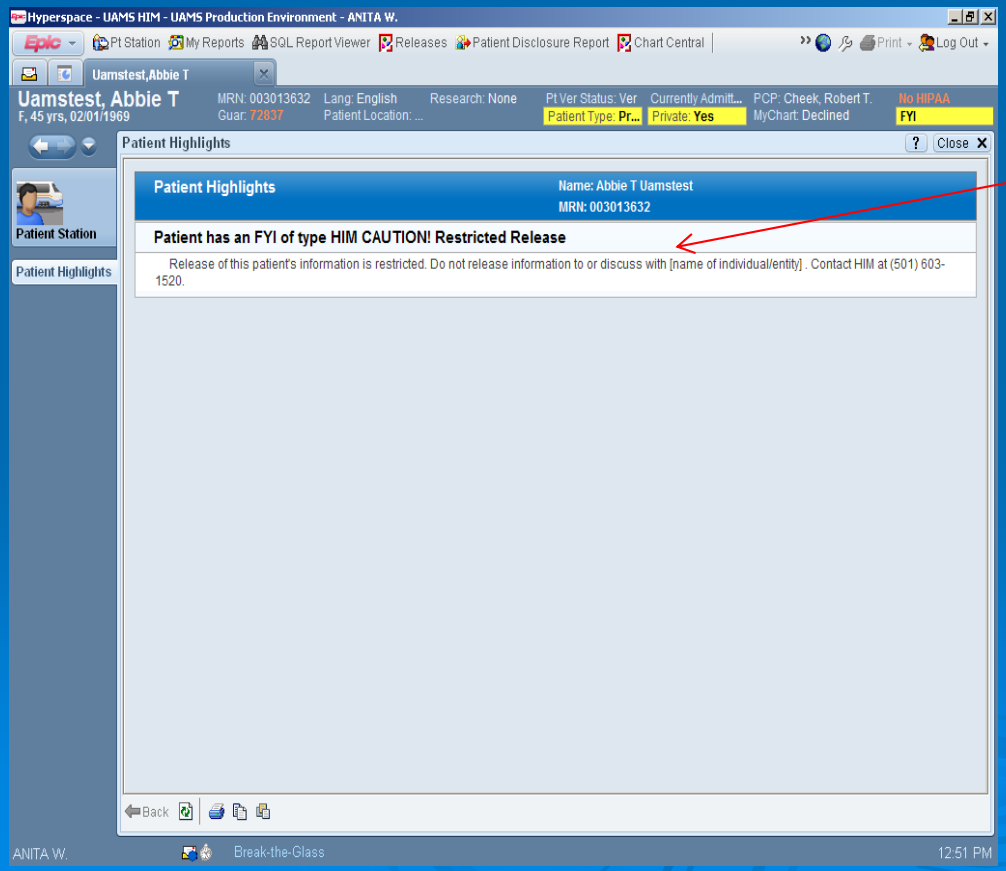
FYI Flag

While UAMS evaluates request



Restriction Requests

If UAMS **agrees** to the request, you would see a "Caution HIM Release Restrictions FYI Flag." Patient Highlights are used to call additional attention to this restriction. Follow the instructions associated with that flag.



Highlights with specific instructions

Legal Representatives

- “the person authorized by law to act on behalf of the patient, such as the parent of a minor or a court-appointed guardian”
- UAMS must treat a patient’s Legal Representative as the patient for purposes of the use and disclosure of the patient’s protected health information

Legal Representatives of Minors

The “Legal Representative” of a minor who has not consented to their own treatment is one who has legal authority to act on behalf of the child, including the authority to make healthcare decisions for the child.

- Parent of minor child
- Father
  - Married to the mother
  - Listed as the father on the birth certificate
  - Court order establishing paternity
- Court appointed guardian of a minor
- A person legally acting as the parent in “Loco Parentis”

Requests by Parents of Minors

- **A divorced parent who does not have custody of the minor child is still the minor's parent, and is entitled to PHI concerning their minor child unless the parental rights have been revoked by court order.**
- **Check for documentation in our systems that the requestor is the parent.**

If Documentation is not Available

- **Explain that information may only be released to the parent or other legal representative.**
- **Ask the requestor to provide a copy of the child's birth certificate which documents their relationship, other legal documentation or have the parent or legal representative who is in the record sign an authorization for the release.**

Legal Representatives of Adults

- Court-appointed guardian of an elderly or incapacitated person;
- Appointed by the patient to act as their attorney-in-fact in a Durable Power of Attorney with health care rights;
- Appointed by the patient in a Health Care Proxy
- Read the documents carefully to make sure they are actually in effect

Legal Representatives - continued

- For other examples, regarding persons of unsound mind, permanently unconscious or terminally ill, or other incapacitated persons see section 5 - Disclosures to Patient's Legal Representatives, - in the Use and Disclosures of PHI Policy 2.1.13 in the Administrative Guide.
- Court-appointed Administrator or Executor or Personal Representative of the Estate of a deceased patient.

  A guardianship or a power of attorney (or any other grant of authority by the patient) are no longer effective upon death. No will is effective until probated.

Personal Representatives – Deceased Patients

Unless an unexpired Authorization signed by the patient prior to death is available, release only to **legal** representative:

- The parent of a deceased minor
- A person (legal entity) authorized by Arkansas law to act on behalf of the estate
  - Must have a court document (remember a will is not effective until probated)
- If caller is not legal representative, refer to reference guide for information that can be released to a family or friend of a deceased patient who is calling for payment purposes and has the account number or medical record number.

Breaches and Breach Reporting

Real Life Example

An employee of a large hospital accidentally left a scheduling sheet containing the information of 192 patients on a subway train. The records were never recovered.

The hospital settled with the OCR for $1 million

What is a Breach?

Any use or disclosure of PHI that is not permitted by the Privacy Rule that poses a significant risk of financial reputational or other harm. For example:

- A UAMS employee accesses the record of a patient outside the performance of their job duties.
- PHI is sent to the wrong fax, mailing address or printer

Notification Requirements

- UAMS must notify every person in writing whose unsecured PHI has been breached as soon as feasible but within 60 days.
- UAMS must report breaches to HHS.
  - If less than 500 individuals, log and report annually.
  - If more than 500 individuals must notify HHS at the same time we notify the patient and we must also notify the media.
- If insufficient contact info for 10 or more patients, UAMS must post on our website

How can you help?

- Notify the UAMS HIPAA Office as soon as you suspect a possible breach. http://hipaa.uams.edu
- The HIPAA Office will then determine if an actual breach has occurred and take care of the notification process.
- Help us keep patient contact information current.
- Follow the workflow for “bad addresses”.
- Follow your department’s documentation requirements.

Take steps to prevent breaches from happening in your department!!

Leaving Messages on Answering Machines or with family members

- Limit the amount of information disclosed to the minimum necessary, such as the provider name and telephone number, or other information necessary to confirm an appointment, or to ask the individual to call back
- Do not leave messages that include test results, or other information that links a patient's name to a particular medical condition or the type of clinic or specialist
- When leaving a message with a family member or friend answering the patient's phone, the message should be limited to a request for the patient to return your call at UAMS/CUMG, your name, and # unless documentation is available to support providing additional information.

UAMS Faxing Policy 2.1.04

- **Confidential** data should be faxed only when mail will not suffice.
- Faxes containing **PHI** and other confidential information must have an official UAMS fax cover sheet.
- Reconfirm recipient's fax number before transmittal.
- Confirm receipt of fax
- Notify your supervisor/HIPAA Office immediately if a fax is sent in error.

Printed PHI

- When retrieving information from the printer and sending information, check every page to make sure it is the correct patient.
- Also make sure other patients' information is not included on the page.
- Don't leave PHI "lying around" where others can see it.
- Don't put PHI in the regular trash. Shred or place in the privacy bins.

Printed PHI

- Check every piece of paper to make sure it belongs to the correct patient before handing, emailing, faxing or mailing information to patients. Examples include:
  - itemized bills
  - statements
- Then double check the email address, postal address or fax number before sending.

Confirm Account

- When working in our systems, always double check that you are in the correct patient's account.
- Examples include, when accepting payments, printing receipts, posting charges, scheduling tests

Verification Assistant (VA) Software

- Verification Assistant (VA) can be helpful to show when a portion of the address has been omitted such as apt number, zip code or if a street number has been transposed.

- If VA shows a completely different address, DO NOT change the address in our system unless you contact the patient directly to verify the address.

Updating Guarantors

- UAMS and our agencies bill by Guarantor.
- Anyone changing insurance to self pay needs to be sure the guarantor information is correct.
- When updating the Guarantor, be sure and update the Guarantor's name as well as the address

Electronic PHI

- Minimize your computer screen if someone walks up
- Log off or lock your computer prior to stepping away from it
- Encrypt any email containing PHI sent outside UAMS intranet by typing secure in straight brackets in subject line [secure].
- All computers and laptops and thumb drives containing PHI must be encrypted.

Passwords

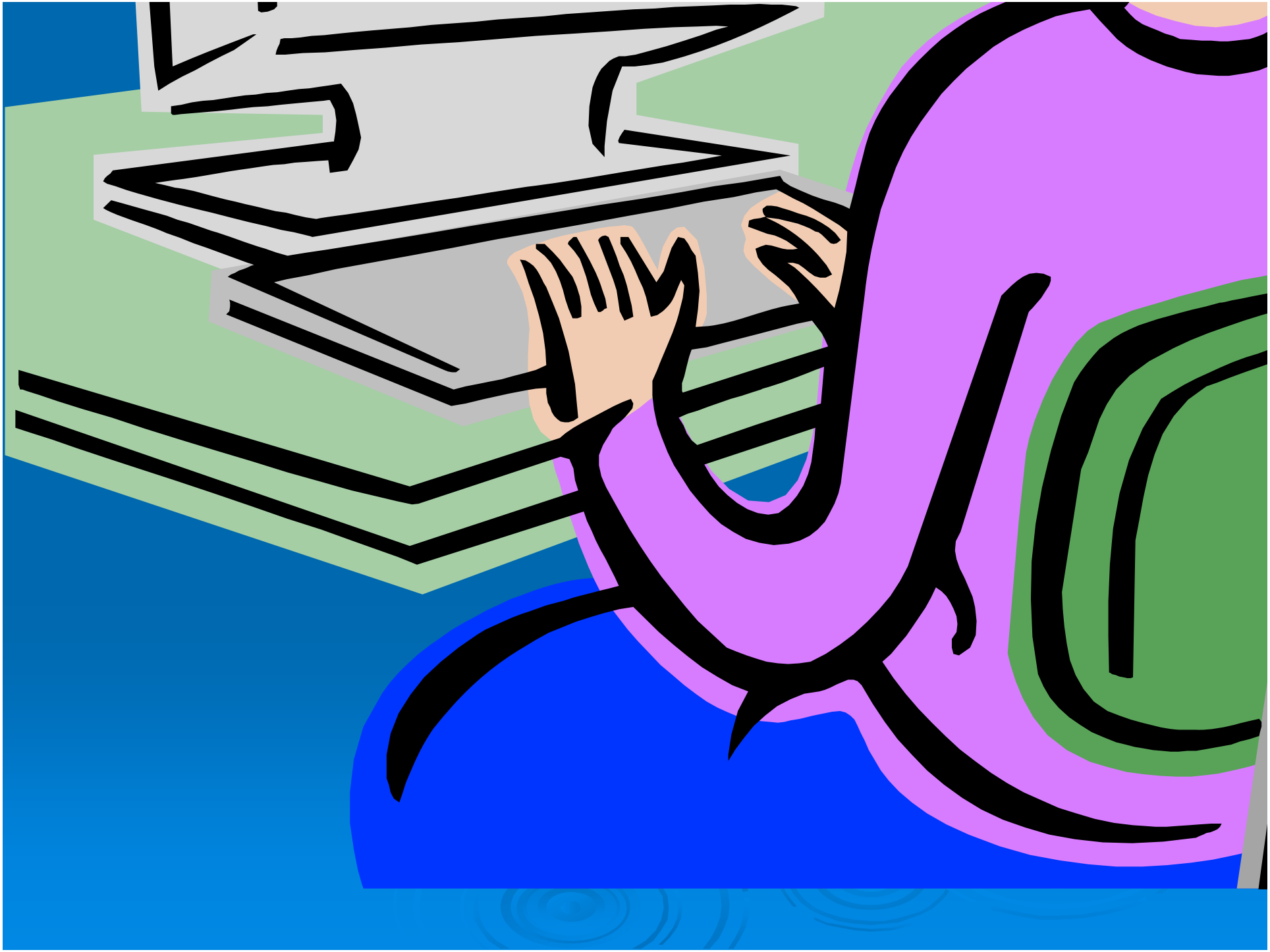
- Always maintain and use passwords in a secure and confidential manner
- Never share your password or use someone else's sign on information
- If you are asked to sign on using someone else's information, refuse to do so and report them

Why would the HIPAA Office call me?

- Access to patient records is monitored
- If your name is on an audit report, and the appropriateness is not readily apparent to the auditors, you or your supervisor will be contacted
- This is routine follow-up and is done for physicians, students and staff.

Why would the HIPAA Office call me?

- Access of patient records outside the performance of your job is prohibited
- This includes your own records and the records of:
  - Family
  - Friends, acquaintances and co-workers
- Violations of UAMS HIPAA Policies are taken so seriously that your supervisor will be notified and must impose disciplinary action
- If we determine the access is a reportable breach, we are required to notify the patient and the OCR



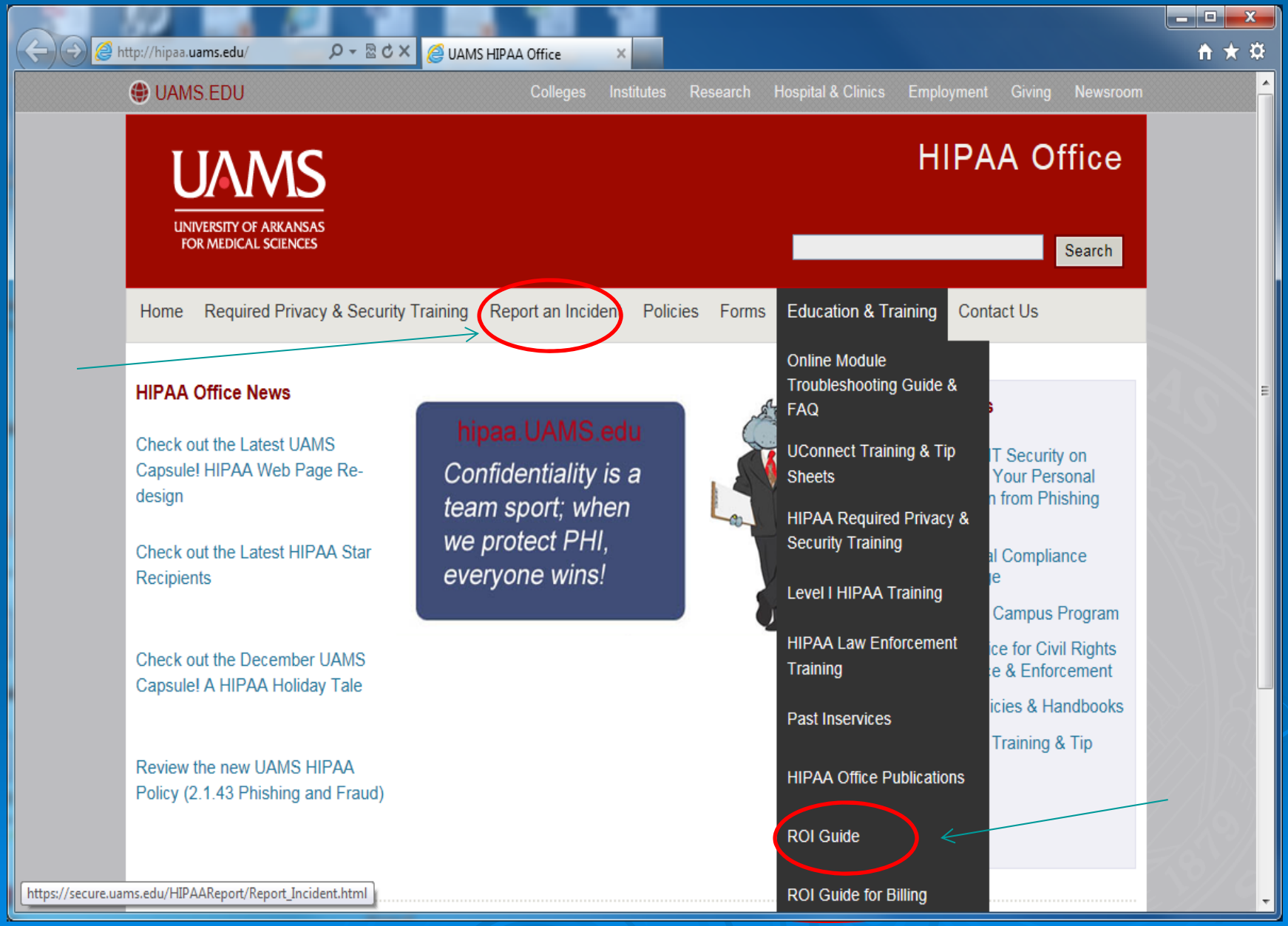
Social Networking

- Do not post photographs, video or any information about a UAMS patient through an electronic means such as social networking sites, blogs, pinging and tweeting.
- The only exception is a response to a UAMS patient that gives no further information about the patient.
- Example of a post that would violate our policy: An employee posts on her face book wall “I talked to a woman today regarding a bill that is almost a million dollars for a ____surgery that she had in March. I would hate to be her.”

Your HIPAA Office

http://hipaa.uams.edu
hipaa@uams.edu
(501) 603-1379

- Heather Schmiegelow– HIPAA Campus Coordinator
- Stephen Cochran – Security Officer
- William Dobbins– Compliance Audit Manager
- Brittany Parker – HIPAA Office Manager/Education Coordinator
- Sara Thompson– HIPAA Compliance Manager & Regional Programs Privacy Officer
- Anita Westbrook– UAMS Medical Center Privacy Officer


http://hipaa.uams.edu/
UAMS HIPAA Office
UAMS.EDU
Colleges
Institutes
Research
Hospital & Clinics
Employment
Giving
Newsroom
UAMS
UNIVERSITY OF ARKANSAS FOR MEDICAL SCIENCES
HIPAA Office
Search
Home
Required Privacy & Security Training
Report an Inciden
Policies
Forms
Education & Training
Contact Us
Online Module Troubleshooting Guide & FAQ
UConnect Training & Tip Sheets
HIPAA Required Privacy & Security Training
Level I HIPAA Training
HIPAA Law Enforcement Training
Past Inservices
HIPAA Office Publications
ROI Guide
ROI Guide for Billing
HIPAA Office News
Check out the Latest UAMS Capsule! HIPAA Web Page Re-design
Check out the Latest HIPAA Star Recipients
Check out the December UAMS Capsule! A HIPAA Holiday Tale
Review the new UAMS HIPAA Policy (2.1.43 Phishing and Fraud)
hipaa.UAMS.edu
Confidentiality is a team sport; when we protect PHI, everyone wins!
https://secure.uams.edu/HIPAAReport/Report_Incident.html