UAMS

UNIVERSITY OF ARKANSAS
FOR MEDICAL SCIENCES

Family Medicine Residents HIPAA Highlights

May 2016

Heather Schmiegelow, JD

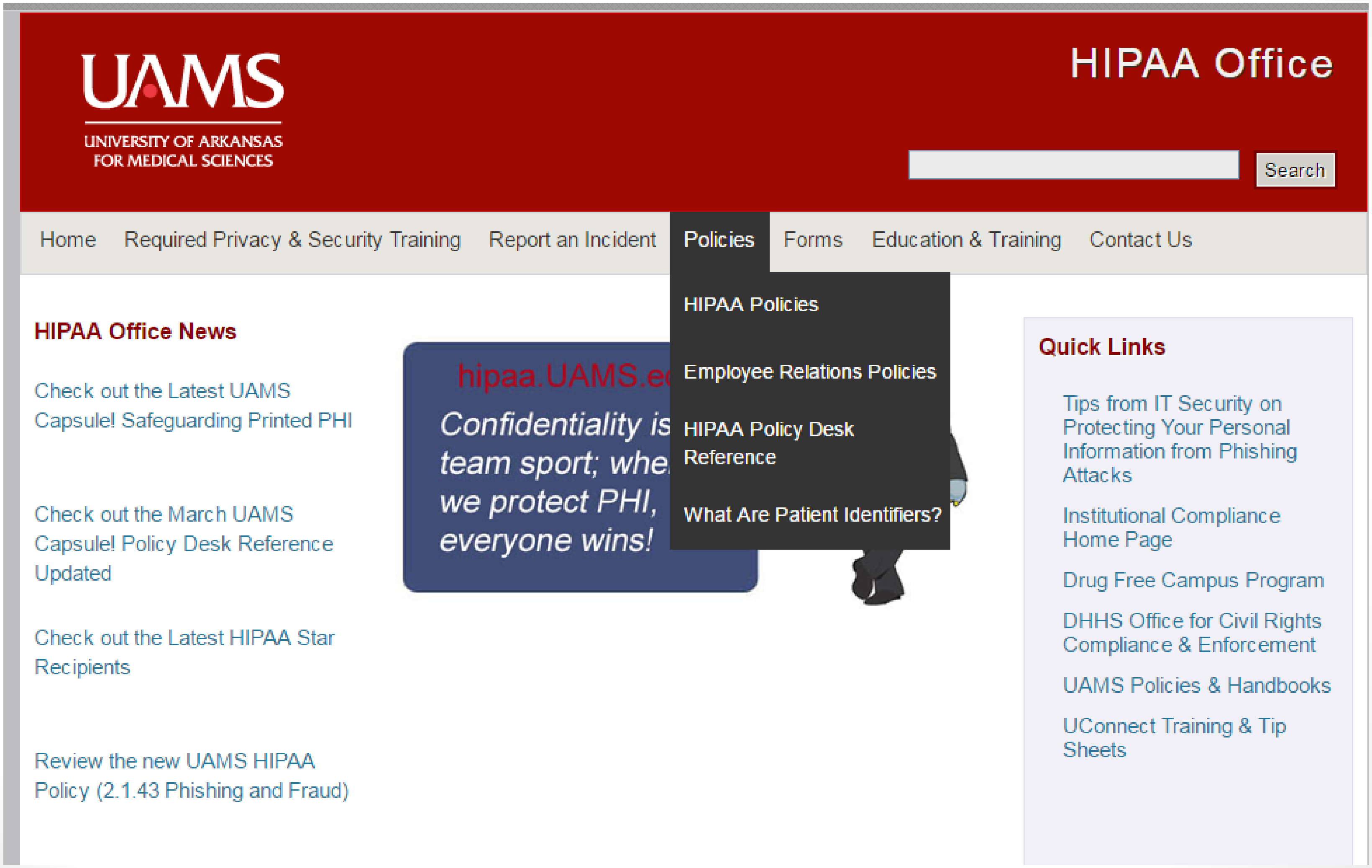
The UAMS HIPAA Office

- Heather Schmiegelow, UAMS HIPAA Privacy Officer
- Stephen Cochran, UAMS Security Officer
- Sara Thompson, HIPAA Compliance Manager
- William Dobbins, HIPAA Informatics Manager & Auditor
- Brittany Parker, Office Manager/Education Coordinator
- Anita Westbrook, Medical Center Privacy Officer
- Jennifer Holland, Research Privacy Officer

http://hipaa.uams.edu

501-603-1379

HIPAA Policies at UAMS



UAMS
UNIVERSITY OF ARKANSAS FOR MEDICAL SCIENCES
HIPAA Office
Search
Home
Required Privacy & Security Training
Report an Incident
Policies
Forms
Education & Training
Contact Us
HIPAA Policies
Employee Relations Policies
HIPAA Policy Desk Reference
What Are Patient Identifiers?
hipaa.UAMS.e
Confidentiality is team sport; whe we protect PHI, everyone wins!

HIPAA Office News

Check out the Latest UAMS Capsule! Safeguarding Printed PHI

Check out the March UAMS Capsule! Policy Desk Reference Updated

Check out the Latest HIPAA Star Recipients

Review the new UAMS HIPAA Policy (2.1.43 Phishing and Fraud)

Quick Links

- Tips from IT Security on Protecting Your Personal Information from Phishing Attacks
- Institutional Compliance Home Page
- Drug Free Campus Program
- DHHS Office for Civil Rights Compliance & Enforcement
- UAMS Policies & Handbooks
- UConnect Training & Tip Sheets

What You Already Know

- HIPAA does not interfere with treatment of patients.
- HIPAA does not interfere with education.
- Never access patient records unless it is part of your job to do so.
- Do not speak about patients in public areas, lower your voice, be aware of who is around you.
- When printing documents containing PHI to shared printers, make sure each page pertains to the correct patient
- Be careful when handling paper documents containing patient information (for example, patient rounding lists). Do not carry them off campus in your lab coat or leave them laying around a resident workroom. Lock them up or shred them! Never leave patient information in a vehicle unattended.
- Log off or lock your computer when you are not using it

Some Things to Be Extra Careful About

- Emails containing PHI must be secure and encrypted
- Emails containing PHI sent from a UAMS email address to another UAMS email address are automatically secure and encrypted
- Emails sent outside of UAMS are **not** automatically secure and encrypted
- To encrypt an email sent outside of UAMS, click on the "mark secure" button provided on the standard toolbar in Outlook or typing the word [secure] in brackets in the subject line will also encrypt the email
- Make sure you are sending the email to the intended recipient
- Include only the minimum necessary PHI in the email to accomplish the intended purpose

Some Things to Be Extra Careful About

- Text messages containing PHI must be secure and encrypted
- Cortext is the app approved by UAMS for secure text messaging
- Contact the UAMS Technical Support Center to get Cortext on your smart phone:

  Phone: 501-686-8555

  E-mail: TechSupportCenter@uams.edu

  Web site: https://uams.service-now.com/ess/

Phishing Attacks

- Phishing attacks are attempts by criminal hackers to obtain UAMS information and use it for criminal purposes, such as filing a fraudulent IRS tax return, submitting false claims for reimbursement to commercial and government payers, and obtaining the payroll funds of a UAMS employee, faculty or staff member
- Be suspicious of emails or other electronic communications from senders you do not know or from senders who do not normally send you such communications
- Do not open an attachment in an email that looks suspicious
- Guard carefully your sensitive information (user ID, password, bank account number, SSN); do not provide it when such information is requested via email

Phishing Attacks

Examples of phishing attacks:

- Click here to receive your 5% raise
- Log in here to increase your email storage capacity
- Click here to obtain your $1,000.00 refund

If you suspect you have received an email that is a phishing attack:

- Report suspected phishing attacks to UAMS IT Technical Support Center at (501-686-8555) or through the IT self-service portal at http://itss.uams.edu; **and**
- Forward the suspect email to ITSecurityTechnical@uams.edu

Some Things to Be Extra Careful About When Using Electronic Devices

- Patient information may never be stored on unencrypted devices. Thumb drives, smartphones, iPads, etc. must be encrypted if they contain PHI – to purchase encrypted mobile devices, submit requests to UAMS IT Technical Support Center at (501-686-8555) or through the IT self-service portal at http://itss.uams.edu
- Cloud storage such as Dropbox, Google Docs, iCloud or any other similar services not authorized by UAMS must never be used for storage or transmission of ePHI .
- Photography of patients in governed by policy – never take a photograph containing a patient, or a part of a patient, or a patient’s name on a piece of paper or computer screen, without consulting the Patient Photography Policy.
- Posting PHI on social media sites like Facebook – do not do it.

Posts about PHI on Social Media Sites Violate HIPAA!

Electronic Public Displays of patient information without a written patient authorization are prohibited. This includes the posting of photographs, video or any information about a UAMS patient through electronic means including, but not limited to, social networking sites; such as Facebook, Twitter, Instagram, blogs, and similar services. The only exception is a posting in response to a UAMS patient that gives no further information about the patient.

Posts about PHI on Social Media Sites Violate HIPAA!

Mary, using her personal iPhone, took digital photos of a patient who had been attacked by a shark. She posts the photos to her Facebook page and includes the following: "You won't believe the shark bite this surfer survived today!" Later that same day, in response to a "Friend's" question, Mary responded: "We were able to save both of his legs." Meanwhile, one of Mary's Friends, "John," responded to Mary's original post with the comment "Yes, that surfer got a lucky break!"

It's important for you to know:

- Mary's profile states that she is a Resident in the Department of Emergency Medicine of Large Hospital System in Anytown, USA; and
- Among her "Friends" is "John," a Resident in the Department of Surgery at the same hospital.

Was this a HIPAA violation? YES!!!!

Some Things to Be Extra Careful About When Talking About Patients

- HIPAA allows you to discuss patient information with “friends and family involved in the patient’s care”
  - If the patient is present or available, obtain their permission first
  - In the patient is not present or available, share only if in the best interest of the patient
  - Use professional judgment to determine if sharing information is appropriate and share only the minimum necessary
  - Be very careful when discussing sensitive information such as HIV status with or in front of family members or friends
- Be careful when discussing patients with each other
  - Do you know your HIPAA identifiers?
  - Do you know who is standing behind you at Doc Java?

Breaches

- UAMS must notify patients in writing of breaches of their PHI
- UAMS must report breaches to the Office for Civil Rights of the U.S. Department of Health and Human Services
- In some cases breaches must be reported to the media
- Examples of potential breaches:
  - an unencrypted laptop containing PHI is lost or stolen
  - an unencrypted thumb drive containing PHI is lost or stolen
  - a rounding list is left in a patient's room
  - an After Visit Summary is given to the wrong patient
  - an email containing PHI is sent to the wrong recipient

Examples of HIPAA Violations Resulting in Monetary Fines

- Feinstein Institute for Medical Research in New York fined $3.9 million related to a laptop computer containing the electronic protected health information (ePHI) of approximately 13,000 patients and research participants stolen from an employee's car.
- Cornell Prescription Pharmacy in Denver, Colorado fined $125,000 regarding the disposal of unsecured documents containing the PHI of 1,610 patients in an unlocked, open container on Cornell's premises.

Call Us or Visit Us Online!

UAMS HIPAA Office

- **Phone: 501-603-1379**
- **Online at http://hipaa.uams.edu**