BREACH REPORTING AND SAFEGUARDING PHI

UAMS DENTAL CLINIC
JUNE 3, 2016

UAMS HIPAA OFFICE

WHY HIPAA MATTERS

- HIPAA is a federal law that protects the privacy and security of patients' health information.
- 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"

WHAT IS PROTECTED HEALTH INFORMATION?

PHI is any individually identifiable information, that an entity governed by HIPAA collects, creates, or receives, that relates to:

- past, present or future physical or mental condition
- healthcare provided or
- payment for care

PHI IDENTIFIERS – 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
- Finger or voice prints
- Medical Record Number
- Health Plan Beneficiary Number
- Account Number
- Certificate/License Number
- Any vehicle or device serial number
- Internet Protocol (IP) Address
- Photographic images
- Web URL
- Any other unique identifying number, characteristic, or code (whether generally available in the public realm or not)

WHAT IS A BREACH?

Any acquisition, access, use or disclosure of PHI that is not permitted by the Privacy Rule that compromises the security or privacy of the PHI

For example:

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

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

BREACH 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 your supervisor or the UAMS HIPAA Office as soon as you suspect a possible breach.
- The HIPAA Office will then determine if an actual breach has occurred and take care of the notification process.
- Learn from the error. Change procedures or practices, as needed, and assist in correcting or recovering from the error ONLY if instructed to do so.
- Don't try to cover it up or "make it right" on your own.
- Help us keep patient contact information current.
- Follow your department's documentation requirements.
- Take steps to prevent breaches from happening in your area!!

PATIENT IDENTIFICATION

- Obtain photo identification if at all possible
- If patient is a minor, document identity of both parents in our system when possible
- 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? "

PATIENT IDENTIFICATION

- National Patient Safety Goal
  - Use at least two patient identifiers when providing care, treatment and services.

- UAMS Patient Identifiers
  1. Name – ask the patient for their full name
  2. Date of birth – ask the patient for their full DOB

- Ask for Patient Name and Date of Birth at EVERY Point of Care, for example scheduling appointments, checking patients in and out, and collecting payments.

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 or after visit summaries, posting charges, scheduling appointments, ordering tests and documenting in the record.

SAFEGUARD PRINTED PHI

- When retrieving information from the printer or fax machine and sending information, check every page to make sure it is the correct patient.
- Make sure other patients' information is not included on any page.
- Check every piece of paper to make sure it belongs to the correct patient before handing or mailing information to patients. Examples include:
  - After visit summaries
  - Prescriptions
  - Appointment information
- When mailing information, make sure the name matches the name on the envelope.

SAFEGUARD PRINTED PHI

- 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.
- When PHI is in transit, place the documents in sealed sleeves, bags or envelopes clearly addressed to the recipient.
- Do not remove PHI from UAMS without managerial approval.
- Check your pockets to ensure you are not taking patient information home

COMMUNICATE QUIETLY

- Make it a habit – always lower your voice when discussing patient information.
- Try to discuss patients privately.
- Stop the conversation if someone walks up.
- If you overhear PHI, keep it to yourself.

LEAVING MESSAGES ON ANSWERING MACHINES

- 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. For example, when confirming an appointment, the information should be limited to appointment date and time, the doctor's name, and a contact name and telephone number.
- Do not leave messages that include information linking 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 your name, phone number, and a request for the patient to return your call at UAMS.

WHEN INVOLVED FAMILY/FRIENDS ASK FOR INFO

- If the patient is present or otherwise available, ask the patient's permission or give them an opportunity to object or infer from circumstances that the patient does not object.
- If the patient is not available or family is calling by phone, follow your clinic's workflow to determine if the patient has identified the requestor as someone who can receive information about them.
- If yes, verify identity and provide info directly relevant to their involvement in the patient's care
  - Note: If the patient is not available or is incapacitated, or in an emergency situation, professional judgment may be used to make the disclosure if you determine it is in the patient's best interest and the patient has not otherwise restricted information to the requesting party.

PATIENT RIGHTS
RESTRICTION REQUESTS 3.1.34

- 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 clinic procedure for making staff aware of any restriction we agree to.

REQUESTS FOR RECORDS

- With a few exceptions, patients or their legal representatives, have a right to access or receive copies of their medical record, including billing records, within 30 days of requesting them.
- Patients have a right to electronic copies of their records.
- If the patient is requesting that family or another designee view or have a copy of the patient's record, a written request from the patient is required.

ELECTRONIC PHI

- Position your monitor so the screen cannot easily be seen by passersby
- Minimize your computer screen if someone walks up
- Log off or lock your computer prior to stepping away from it
- All computers and laptops and thumb drives containing PHI must be encrypted

PASSWORDS

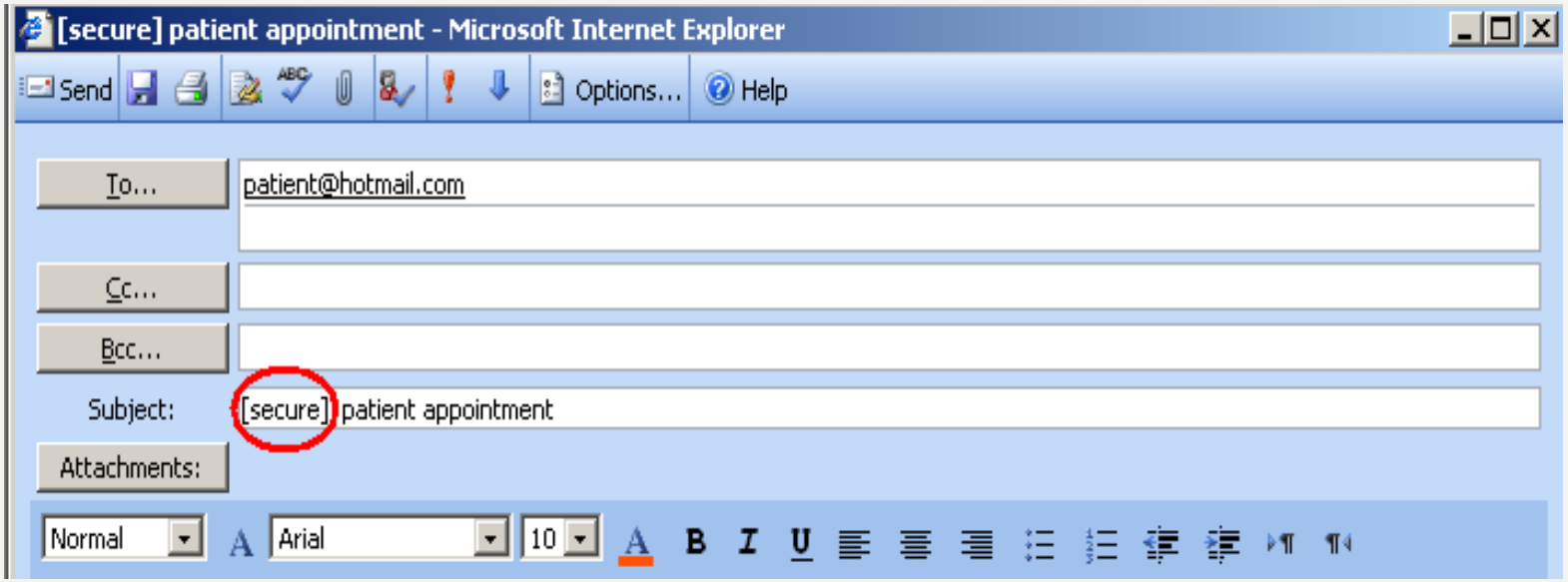
- Always maintain and use passwords in a secure and confidential manner
- Never share your password or use someone else's sign on information
- If you are asked to sign on using someone else's information, refuse to do so and report them

UAMS E-MAIL POLICY

- UAMS e-mail resources are for official UAMS business only.
- Some guidelines for e-mailing **PHI** and confidential information include:
  - Limit the PHI provided to the minimum necessary.
  - Do not send PHI to a personal email account.
  - Be careful how you "say things" in e-mails and do not e-mail extremely sensitive information.
  - 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 e-mails that may contain confidential information.

EMAIL CONTAINING PHI MUST BE ENCRYPTED

- Emails sent from one UAMS email account to another UAMS email account are automatically encrypted.
- Use the encryption feature of the UAMS e-mail system when sending e-mail outside the UAMS domain by typing [secure] into the 'subject' field of the message.



UAMS FAXING POLICY

- **Confidentia**l 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.

SOCIAL NETWORKS ARE NOT PRIVATE!

- Remember that when you are communicating with someone via IM, Facebook, Twitter, etc., NONE of these things are private.
- You should *never* discuss patient care via these methods, even if you believe you have de-identified the patient information.
- UAMS policy prohibits the posting of any information about patients on websites, including Facebook and other social media sites.
- Violation of this policy will result in disciplinary action up to termination.

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 clinicians, 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

Penalties for HIPAA Violations- Disciplinary Notice Policy & US Government Sanctions

UAMS HIPAA Sanctions Policy 2.1.42 in the Administrative Guide

Violations by UAMS Workforce will result in disciplinary action, up to and including termination from employment with UAMS.

Civil/Criminal penalties:

In addition, you can be subject to civil and criminal penalties imposed by the federal government up to $1.5 million and 10 years in prison.

Recent Enforcement Activities of the Office of Civil Rights

- $4.8 million fine - physician attempted to deactivate a personally-owned computer server that resulted in electronic protected health information (ePHI) being accessible on internet
- $4.3 million fine – organization violated 41 patients' rights by denying them access to their medical records
- $1,725,220 fine - an unencrypted laptop was stolen from facility
- $1.7 million fine – ePHI of 612,402 individuals accessible to unauthorized individuals over the Internet
- $865,500 fine - employees repeatedly and without permissible reason looked at the ePHI of ***celebrity*** patients
- $800,000 fine – employees left 71 cardboard boxes of medical records of more than 5,000 patients in the driveway of the physician's home

REPORTING POTENTIAL VIOLATIONS

- All known or suspected HIPAA violations or breaches must be reported.
- There will be no retaliation for good faith reporting.
- Reports can be made to:
  - Reporting line at 1-888-511-3969
  - HIPAA Office at 501-614-2187
  - Incident Report Link online at hipaa.uams.edu
  - Anyone in a position of responsibility - the person receiving the report should then contact the HIPAA Office.

YOUR HIPAA TEAM

- Heather Schmiegelow, UAMS HIPAA Campus Coordinator (501-526-4817)
- Anita Westbrook, Medical Center Privacy Officer (501-526-6502)
- Jennifer Holland, Research Privacy Officer (501-526-7559)
- Tracy Petty, PRI Compliance Officer (501-526-8177)
- Steve Cochran, Security Officer (501-603-1336)
- Bill Dobbins, Informatics Manager & Auditor (501-526-7436)
- Sara Thompson, HIPAA Compliance Manager (501-614-2098)
- Brittany Parker, Education Coordinator (501-603-1379)

WWW.HIPPA.UAMS.EDU

QUESTIONS?

If you have questions or concerns, contact the HIPAA Office, or the HIPAA hotline at:

(501) 603-1379

1-888-511-3969

www.hippa.uams.edu