Protecting Patient Privacy

Eugene A. Lewis, D.C., M.P.H.
for the North Carolina Chiropractic Association

As health care workers we see and hear confidential information every day and are entrusted with patient health information, but solely to be of service to that patient.

Distinguishing Between Privacy and Confidentiality

- **Privacy** is about access to and or control over a person
- **Privacy** is being free from being observed or disturbed by other people
- **Confidentiality** is about control over information, how it is shared and who gives the authority to share it
- Much of what is called “privacy” protection is really about confidentiality.

Confidentiality and Privacy

- Having patient information in the system is important for many reasons (research, controlling disease outbreaks, treatment)
- This information may not get into the health care system unless people trust whoever has it
- Depending on the situation, we may need to protect confidentiality to protect privacy (or the reverse)

Confidentiality and Patient Trust

- Over 16% of patients withhold information from providers because of concerns about whether it will be protected
- Almost 10% of patients chose not to participate in a Massachusetts EHR project, with many citing privacy concerns
- Polls about using patient health information in research revealed that 28% said they wouldn’t give consent to release information and 13% refused to participate or be contacted
- 12.5% admitted lying to their doctors about symptoms or behaviors, refusing to provide information, providing inaccurate information, paying out of pocket for care that is covered by insurance or avoiding care because of fears of privacy intrusion

1 California HealthCare Foundation, National Consumer Health Privacy Survey 2005
3 Harris Interactive (2007); Research!America Volume 7 (2007)
• The use of electronic health records in health care will continue to grow
• Patient confidentiality concerns are significant
• If patients are to trust providers’ use of EHRs, it will be important to avoid “surprises” about their health information

Areas of Concern
• Protection of categories of sensitive information as records are transmitted among providers
• Entities outside of health care and data transfers to them, even at patient request
• “Data mining”
• Syndromic surveillance and disease reporting

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

What is HIPAA and What Does it Govern?
A multifaceted regulation covering three areas
• Insurance portability
• Fraud enforcement (accountability)
• Administrative simplification (reduction in health care costs)
  a) privacy
  b) security

Why HIPAA?
• The U.S. previously replied on patchwork of laws to protect patient information and it could be distributed without notice or consent and for reasons that had nothing to do with a patient’s medical treatment or reimbursement
• With information held and transmitted electronically, the old system of paper records in locked filing cabinets is not enough

HIPAA
• Protects all health information created by a healthcare provider, health plan or healthcare clearinghouse
• Protects this information no matter how it is transmitted (verbally, electronically or in writing)
• Defines who is allowed to use patients’ protected health information
Common HIPAA Jargon

- **IIHI** - Individually Identifiable Health Info
- **PHI** - Protected Health Information
- **CE** - Covered entity
- **TPO** – treatment, payment and operations (healthcare)
- **NPP** - Notice of Privacy Practices

Who in the Healthcare Workforce is Covered by HIPAA?

- Most providers: hospitals, doctors, NP’s, PA’s and other providers, laboratories, nursing homes, pharmacies and others
- Payor clearinghouses
- Health plans
- Almost anyone connected with health care delivery

Am I Part of the Workforce?

You are part of the workforce if you are a
- Physician
- Employee
- Volunteer
- Contractor (if possibility of access to PHI)
- Consultant (if possibility of access to PHI)
- Student in a healthcare rotation or observing at a healthcare facility

Third Party Contractors / Business Associates Are Also Covered

A person (vendor) who performs or assists a provider or health plan in the performance of
- A function or activity involving the use or disclosure of PHI, or
- Any other function or activity regulated by the HIPAA Privacy Rule

“Business Associates”

- Transcription services
- Coverage doctors
- Temporary employees
- Utilization review contractors
- Sales representatives who have access to patient information, such as software vendors

Must sign confidentiality agreement

Who is *not* a business associate

- Delivery services
- Repair / service personnel (unless they have access to patient records on computer)
- Cleaning crews
HIPAA protects individually identifiable health information (PHI) that is transmitted or maintained in any form by covered entities.

Protected Health Information (PHI)

- PHI is any health information that is created by or received by a covered entity.
- Relates to the past, present or future physical or mental health or condition of an individual or the past, present or future payment for the provision of health care to an individual.
- The protections apply to the information in any form (verbal, written, etc.).

Protected Health Information (PHI) includes, but is not limited to:

- Medical treatment records and reports
- Bills, receipts, EOBs, etc.
- Labels on items provided to a patient
- Test results
- Patient information on any computer device, including mobile devices
- X-rays, CT scans, MRI’s, BMD’s, etc.
- Facility appointment schedules

What Does HIPAA do for Patients?

- Helps them make informed choices when selecting both health care and payors, based on how PHI may be used.
- Enables patients to know how their PHI may be used and what disclosures of their information have been made.
- Limits release of information to the minimum needed.
- Gives patients right to examine and obtain a copy of their own health records (and request changes, if necessary).
- Holds violators accountable with civil and criminal penalties.
- Strikes a balance when public responsibility requires disclosure (to protect public health, for example).

What Does HIPAA Mean for Providers?

- Requires providing information to patients about privacy rights and how their PHI can be used.
- Requires adopting clear privacy procedures for their health care facility.
- Requires employee training about privacy procedures.
- Requires designating an individual responsible to see that privacy procedures are adopted and followed.
- Requires securing patient records so that they’re not available to those who do not need them.

Individually Identifiable Health Information (IIHI)

- All information which may identify a patient (there are 19 items).
- IIHI is protected under the law.
- 10 most common: name, address, phone number, DOB, Social Security number, medical record number, relatives’ names or other information, employer, insurance ID number.
What is Deidentification?

• Deidentified data is usually created by removing all 19 identifiers from a patient’s health record
• Often done for research or teaching purposes

Authorization is required for the use and disclosure of health information

Authorizations

• Signed permission from patient or legal guardian to release PHI (keep on file)
• Must be obtained where PHI is used for other than TPO
• Is time limited (by a date)
• May be revoked by patient
• Lists what and to whom PHI will be sent
• If someone is retrieving records for patient, must be an authorization allowing it and person must also present ID (copy it)
• Make a dated note in the chart that records were sent, picked up, etc.

Accounting for Disclosures

Upon request, covered entities must disclose to patients within 60 days to whom information has been shared except

• Instances when the information is disclosed to the individuals themselves
• When it was used for TPO
• Under a specific authorization (medical examiner, police, public health agency, etc.)

A patient can say it’s permissible to share information with other family members but be sure to document that you received at least verbal approval (preferably written approval)

Notice of Privacy Practices (NPP)

• Describes ways a healthcare facility may use PHI
• Describes rights patient has to protect their PHI
• Describes the duties of the healthcare facility to protect patient’s PHI
• Informs patient about complaint and investigation process if breach occurs
• NPP must be given to and signed by patient before the first encounter
Ways to Protect Patient Privacy

- Close patient room doors when discussing treatments and administering procedures
- Speak quietly when conversations might be overheard
- Avoid discussions about patients in public places
- Don’t leave messages regarding patient conditions or test results on answering machines or with anyone but the patient

Ways to Protect Patient Privacy

- Avoid speaking to patients in public using information that could reveal their health issues. “Hi, Bob! How’s that ‘ol back pain doing?”
- Don’t leave records unattended in an area where others can see them
- When finished using PHI return to its appropriate location
- When finished looking at electronic PHI log off the system
- Don’t leave information visible on an unattended computer monitor (including daily schedule)

Ways to Protect Patient Privacy

- For door slots, turn patient folder so that names are not visible
- Cover appointment lists
- Sign-in sheets need permission to expose patient names to others
- Patients on “thank-you” and birthday reception room boards need to grant permission first
- When discarding paper PHI make sure the information is shredded
- Leave messages, reports or letters for patients in sealed envelopes marked “confidential”

Ways to Protect Patient Privacy

- Keep files closed

Transporting PHI

- When transporting PHI inside or outside the facility, protect it from being seen by others
- Use a container or unmarked envelope if appropriate
- Turn files face down
- Don’t leave records where they can be viewed by unauthorized personnel
- Don’t leave records in break rooms, etc.
- If PHI is found, return it or destroy it

Computers in Healthcare

- Review your organization’s policies on using computers: write rules and make everyone aware of them
- Never use facility computers to access unknown websites or open attached files from an unknown source
- Send and store information on public networks only in encrypted form
Computers in Healthcare

- Implement procedures by which it is possible to identify the senders and recipients of data and that they are authorized to receive and decrypt the information
- Computers with patient information have to be password-protected (only staff with “need to know” gets the password)
- If taking a computer or storage device with patient information out of the office, it also has to be password-protected
- Position the monitor screen so it can not be easily viewed by passers-by as you are working

Emails

- Do not use work e-mail for personal messages
- Never send confidential PHI in an e-mail unless your facility has mechanisms in place to protect the information
- Always double-check the address line of an e-mail before you send it
- Emails to and from patients about their care become part of the patient record

Faxes

- Fax is a poorly controlled communication
- When faxing PHI, use a cover sheet (without patient name)
- Verify the correct destination fax number
- Verify that the receiving fax unit is in a secure location or the receiving person is available to receive the fax when sending PHI
- When receiving faxed patient information, immediately remove it from the machine and deliver it to the recipient
- If information has been faxed to your facility in error, immediately inform the sender, and destroy the information

Fax Confidentiality Notice

The information contained in this facsimile is privileged and confidential information and may contain information that is protected under 42 U.S.C., 1301. The information contained herein is intended for the use of the individual or entity named above. If the reader of this message is not the intended recipient, or the employee or agent responsible to deliver it to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this information is strictly prohibited. If you have received this communication in error, please immediately notify us by telephone at (999) 123.4567. Thank you.

Exceptions to Privacy Rights

- Laws that require providers to report certain communicable diseases to state health agencies when patients have these diseases, even if the patient doesn’t want the information reported
- North Carolina requires health workers who suspect child abuse or domestic violence to report it to authorities
- Law enforcement, when conducting investigation (must show warrant)
- Employers in certain cases such as workers’ compensation
- Organ procurement organizations
- Medical examiner, coroner, funeral director

Minors

- A minor child (under age 18 in North Carolina) cannot obtain treatment without parental or legal guardian consent
- Only designated parents or legal guardians (information on file) are allowed to be given the minor’s PHI
- Can the minor prevent the designated adult from receiving the PHI? Depends.
What if PHI is Breached?

- What to do should already be in office policy manual
- Reaction depends on seriousness of breach and how many patients involved
- Report immediately to privacy officer
- HIPAA allows 60 day window to act
- Analyze to see if breach needs to be reportable to patient or USDHHS (not all are)

What if PHI is Breached?

- If reportable, have to contact patient by mail/email within maximum of 60 days
- Notify media if > 500 patients
- Notify USDHHS if > 500 patients, including:
  - Who impermissibly used the PHI or to whom was the PHI impermissibly disclosed
  - The type and amount of PHI involved
  - Whether and what immediate steps were taken to mitigate use or disclosure
  - Whether the PHI was returned prior to being used for an improper purpose

Reporting Breach to Patient

Notice must include

- Description of what happened
- Date of the breach and the date of the discovery
- Types of PHI that were involved in the breach
- Steps that patients should take to protect themselves from potential harm from the breach
- List of steps the covered entity is taking to
  - Investigate the breach
  - To reduce further harm to patients
  - To protect against any further breaches
- Contact procedures for patients to ask questions

Breaches of Patient Financial Information

- Credit card or banking information may be obtained by unauthorized personnel
- Important to contact patients without any delay
- Health care facility could be made responsible for financial losses

Examples of Data Breaches

- PHI accidentally discarded in trash
- PHI sent in email to wrong recipient
- PHI stolen for monetary gain
- PHI obtained by hackers or computer virus
- PHI lost in stolen laptops or data storage devices
- Copier disposed without being “cleaned”

Not reportable

- Unintentional acquisition, access or use of PHI by an unauthorized person, provided the PHI is not further used or disclosed
- Example: an EOB is accidentally mailed to the wrong patient and recipient notifies doctor’s office and is told to destroy the EOB
If PHI Breached, the Healthcare Facility May Also Want to Contact Malpractice Carrier for Their Instructions and Advice

Reporting Abuses

If a patient, a member of the public, or an employee suspect that an organization is not complying with HIPAA, that person can file a complaint with the Office for Civil Rights (OCR) at the US Department of Health and Human Services.

Breaking HIPAA privacy or security rules can mean either a civil or a criminal sanction:
- Knowingly releasing PHI can result in one-year jail sentence and $50,000 fine
- Gaining access to PHI under false pretenses can result in a five-year jail sentence and a $100,000 fine
- Releasing PHI with harmful intent or selling the information can lead to a 10-year jail sentence and a $250,000 fine

Rural settings sometimes have additional problems of maintaining privacy and confidentiality:
- Interrelated community members
- Familiarity of patients and staff
- More people know each other
- More casual attitude toward formal privacy regulations

When confidentiality isn’t protected:
- Trust is broken
- Interferes with effective care
- Limits ability to obtain an accurate medical history: reluctance to share information
- Reluctance to come to facility for care
- Possible fines & legal action

Strategies:
- Share patient information on a “need to know” basis according to medical necessity
- Does this person really need to know this information to do their job?
- If it was my medical information what would I want?
Phone Conversations

- Avoid discussing patients in areas where you can be overheard
- Talk quietly
- Always identify the person you are talking to

The Reception Area

- Speak to patients about their condition in private rooms, not in the reception area
- It’s permissible to call a patient by name from a waiting room

A famous case

- Country singer Tammy Wynette’s medical records were sold to two tabloids by a hospital employee
- The hospital was sued
- The hospital employee was fined and sent to prison for six months
- The public’s trust in the hospital was damaged, and a patient’s reputation was compromised

What to Say When Asked

- Never share PHI with family or friends
- If asked about a patient, the best simple response is, “I’m sorry, but we’re not allowed to talk about our patients”
- Shows them that you will also not reveal information about them if they become a patient

What about another patient who referred someone and asks how they are doing?

Unless you have permission, you can say nothing

"According to your HIPAA release form, I can’t share anything with you."
Security Risk Assessment (SRA) Tool

- Developed by the HHS Office of the National Coordinator for Health Information Technology
- The SRA tool is a software application that helps small-to-mid-sized providers conduct risk assessments of their organizations