Rural Health Clinic Technical Assistance Webinar

This webinar is brought to you by the National Association of Rural Health Clinics and is supported by cooperative agreement UG6RH28684 from the Federal Office of Rural Health Policy, Health Resources and Services Administration (HRSA). It is intended to serve as a technical assistance resource based on the experience and expertise of independent consultants and guest speakers.

The Latest HIPAA Requirements – A Check-in on Your RHC's Compliance

NARHC Webinar

January 14, 2025

Jennifer Claymon
jclaymon@reedclaymon.com
512-660-5965

Reed, Claymon, Meeker, Krienke & Spurck, PLLC
901 S. Mopac, Suite 290
Austin, TX 78746
512.660.5960 main
512.660.5972 fax
reedclaymon.com

What is HIPAA?

Health

Insurance

Portability and

Accountability

Act of 1996

Reed + Claymon

Amendments to HIPAA

"HITECH" Act

Health Information Technology for Economic and Clinical Health Act of 2009

"GINA"

Genetic Information Non-Discrimination Act of 2009

Reed Claymon

When did HIPAA go into effect?

- Privacy Standards – 4/14/2003
- Transaction Standards – 10/16/2003
- Security Standards – 4/20/2005

Reed + Claymon

HITECH

- Issued rules effective in 2013
  - Added notification of breach
  - Enhanced enforcement
  - Direct liability for Business Associates

Both federal and state governments are paying attention …

Reed Claymon

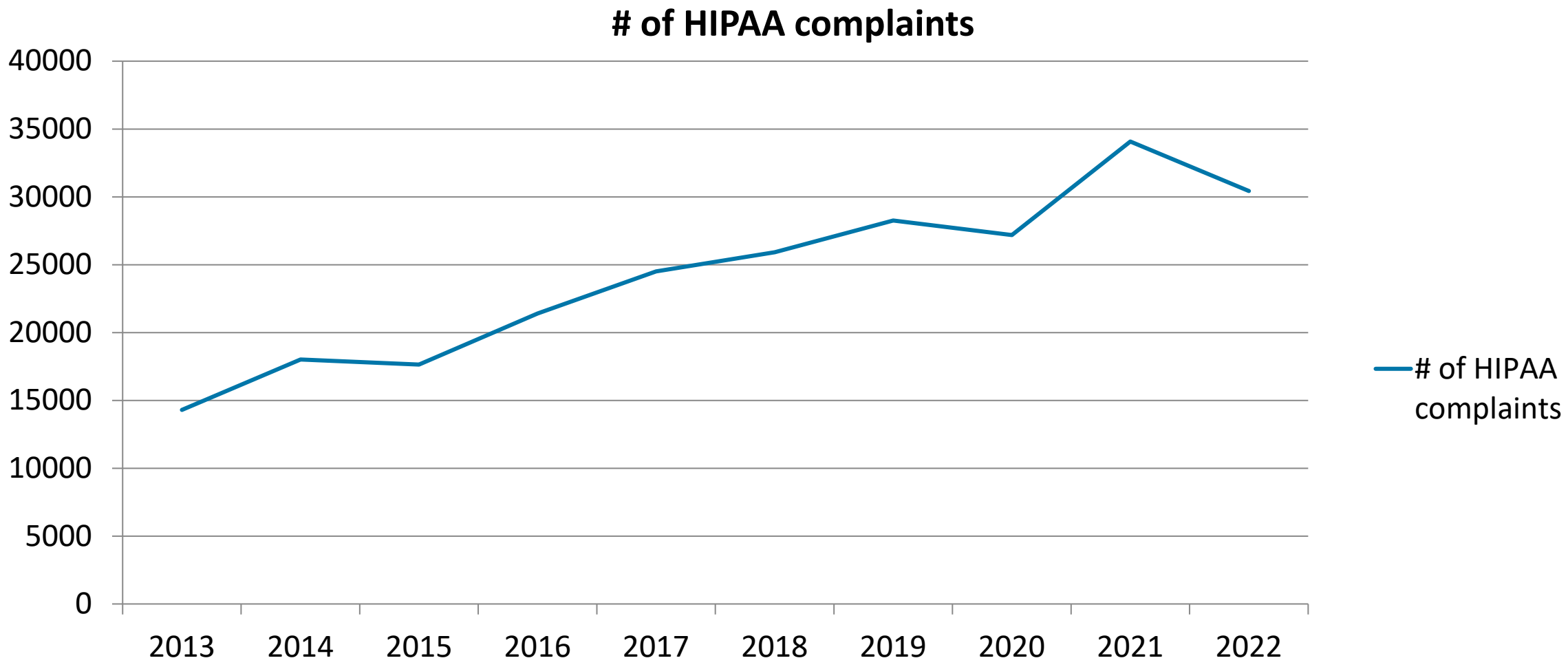
New Era of Enforcement

- Early HIPAA
  - Civil Monetary Penalties (CMP) of $100 per violation
- HITECH
  - Tiered ranges of penalty amounts
  - Criminal violations possible
    - Fines up to $250,000
    - Up to 10 years in prison

Reed + Claymon

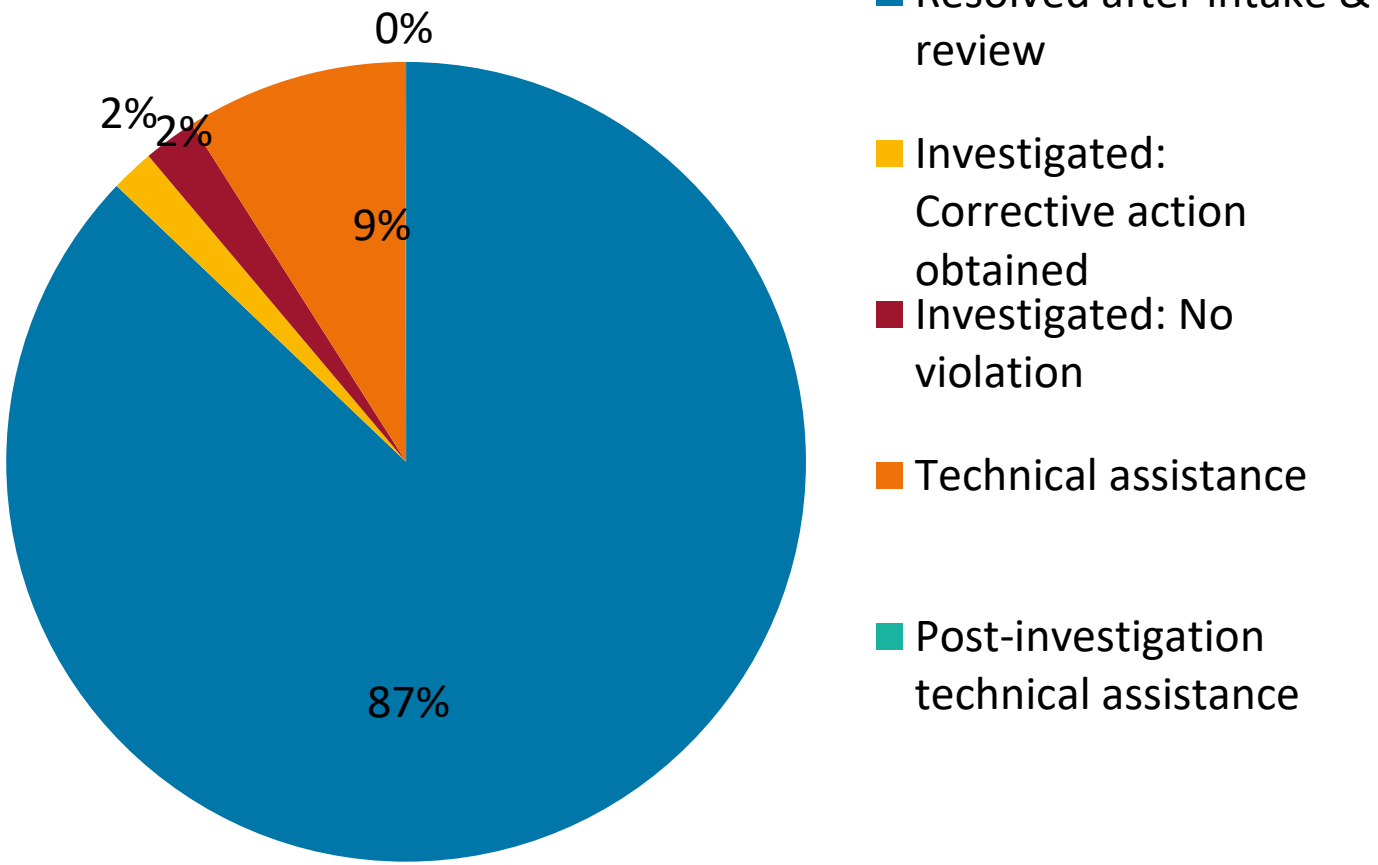
Enforcement

- State Attorneys General
- Can enforce HIPAA
  - Civil action
  - Injunction
  - Damages
- Can enforce state law



Reed Claymon

2022 OCR resolution of complaints



Reed + Claymon

Top 5 Issues in OCR Investigations with Corrective Action - 2022

5. Breach – Notice to Individual
4. Administrative safeguards
3. Safeguards
2. Access
1. Impermissible uses & disclosures

Why are we still talking about this?

Doesn’t everyone know what they are supposed to do?

Reed + Claymon

Recent OCR Settlements

Reed + Claymon

Heritage Valley Health System (PA, OH, WV)

- Ransomware attack
- OCR compliance review after media reports
- Investigation found failures to:
  - Conduct compliant risk analysis of electronic PHI
  - Implement contingency plan to respond to emergencies, like a ransomware attack, that damage systems that contain ePHI
  - Implement policies and procedures to allow only authorized users access to ePHI
- $950,000 and corrective action plan

West Caldwell Care Center (NJ)

- Son requested mother's medical record and provided power of attorney upon request
  - Son and mother were in dispute with NF over payment
- NF did not provide copy of medical record within 30 days of receiving request
  - Provided record 161 days after request (two months after receiving notice of OCR investigation)
- OCR offered opportunity to settle matter informally (please respond within 10 days)
- NF responded 35 days later – acknowledged they didn't provide records but argued with OCR
- CMP of $100,000
  - 161 days at $1,280 per day
  - $206,080 total, but capped at $100,000

Phoenix Healthcare dba Green County Care Center (OK)

- Phoenix Healthcare would not provide personal representative with copy of her mother's medical records
- OCR attempts at technical assistance and attempts to get records
- Sent records 323 days after request
- Settled for $35,000 after hearing before ALJ

Montefiore Medical Center (NYC)

- Hospital employee stole ePHI of 12,517 patients and sold information to identity theft ring
  - Hospital discovered 2 years later after NYPD informed them there was evidence of theft of specific patient's medical information
- OCR investigation found failures to:
  - Analyze and identify potential risks and vulnerabilities to PHI
  - Monitor and safeguard EHR activities
  - Implement policies and procedures that record and examine activity in information systems
- $4,750,000 and corrective action plan

St. Joseph's Medical Center (NY)

- Disclosed COVID-19 patients' PHI to AP for an article about hospital's response to public health emergency
  - Photographs, diagnosis, current medical status and prognosis, vital signs and treatment plans
- Did not obtain written authorization from three patients
- $80,000 and corrective action plan

HIPAA Compliance is Important!

Reed + Claymon

Who must comply with HIPAA?

- Health plans
- Health care providers who conduct electronic billing/transactions
  - Hospitals
  - Doctors
  - Clinics
  - Other providers – PT, OT
- Business Associates
  - Lawyers
  - Consultants
  - Accountants

What does HIPAA do?

- Federal law requiring health care providers and business associates to protect privacy of individually identifiable health information
- Requires health care providers and business associates to adopt policies and procedures on privacy and security
- Requires health care providers and business associates to train workforce on privacy and security

Reed + Claymon

Type of Information Protected

- Protected health information ("PHI")
  - Includes information transmitted or maintained in any form, including all written and oral communications
  - Identity, fact that patient received health care
- Individually identifiable health information
  - De-identified information isn't subject to standards – must remove all 17 identifiers listed in regulations

Authorization

- Basic rule: Except as otherwise authorized by HIPAA, covered entity may not use or disclose PHI without valid authorization
- Use or disclosure must be consistent with authorization

Authorization

- Defective authorizations
  - Expiration date has passed or expiration event has occurred
  - Authorization not completely filled out
  - Authorization is combined with another document
  - TPO is conditioned on authorization
  - Info in authorization is known to be false
- If in doubt, get a new authorization

Permitted Uses and Disclosures – No Authorization Required

- Treatment
- Payment
- Health care operations
  - Quality assurance/performance improvement
  - Credentialing/peer review/evaluations
  - Legal services
  - Audits
  - Business management/planning

Permitted Uses and Disclosures – No Authorization Required

- To individual patient (or authorized representative)
- To business associate

Reed + Claymon

Patient Authorization NOT Required

- Required by law
- Public health activities
- Abuse, neglect of child, disabled or elderly
- Health oversight activities
- Judicial & administrative proceedings
- Law enforcement purposes
- Coroners, MEs, funeral directors
- Organ & tissue donation
- Research approved by IRB
- Serious threat to health or safety
- Specialized government functions
- Worker's compensation

Opportunity to Object Required

- Directory information (hospitals)
- Disclosure to family members and others involved in patient's care or payment for care

Reed + Claymon

Patient's Rights regarding Health Information

- Right to receive a notice of the covered entity's privacy practices
- Right to access his/her own health information
- Right to receive information in electronic format if maintained in electronic format
- Right to request amendment of his/her health information
- Right to receive accounting of disclosures of PHI

Reed + Claymon

Personal Representatives

- Treat personal representative like patient for purposes of HIPAA
- Who is the personal representative for an adult or emancipated minor?
  - Person who has authority to act on behalf of the adult/emancipated minor patient in making health care decisions
    - Medical Power of Attorney
    - Guardianship
    - Incompetent/incapacitated patient

Personal Representatives

- Who is the personal representative for an unemancipated minor?
  - Parent, guardian, other person acting in loco parentis who has authority to act on behalf of minor patient in making healthcare decisions

Personal Representatives

- Who is the personal representative for a deceased patient?
  - If patient had a will → executor/probate administrator
  - If patient did not have a will → any of the heirs (this may vary according to state law)

Minimum Necessary Standard

- Limit info to “minimum necessary to accomplish intended purpose of use, disclosure or request”
- Exceptions:
  - Treatment purposes
  - Disclosure to patient of own PHI
  - Authorization by patient
  - DHHS investigation
  - Required by law

Reed + Claymon

Reproductive Health Information

- Published 4/26/24; effective 12/23/2024
- Prohibits covered entities and business associates from using or disclosing PHI:
  - To conduct a criminal, civil, or administrative investigation into a person, or to impose civil, criminal, or administrative liability on any person, for the mere act of seeking, obtaining, providing, or facilitating reproductive health care
  - To identify any person for any purpose described above

Reproductive Health Information

- Applicable when:
  - The reproductive health care is lawful under the law of the state in which the care is provided and under the circumstances in which it is provided; or
  - The reproductive health care is protected, required or authorized under federal law, including U.S. Constitution, under circumstances provided; or
  - Presumption that care is lawful when care is provided by person other than the entity receiving request for PHI except:
    - Entity has actual knowledge that care was not lawful or factual information from requestor that care was not lawful

Reproductive Health Information

- Entity may release if it receives a valid attestation from the requestor that the use or disclosure is not for a prohibited purpose and statement that person may be subject to criminal penalties for knowingly obtaining or disclosing PHI in violation of HIPAA

Effect of New Administration

- These rules may be withdrawn with the new administration coming into office
- Until they are withdrawn, they are in effect unless there is a court order to the contrary
  - There is a limited injunction in Texas applicable only to the plaintiff provider who filed the suit

Notice of Privacy Practices

- Update your notice of privacy practices!
- Specific changes from 4/24/24 final rule
  - Reproductive Health
  - Part 2 (substance abuse treatment) records

New Proposed Security Rules

- Published 1/6/2025; comment period for 60 days
- First change to security rules since 2013
- Specifically notes need for small and rural healthcare providers to implement strong security
- Applies to covered entities and business associates

New Proposed Security Rules

- Some of the notable changes
  - Multi-factor authentication
  - Annually assign risk levels to threats
  - Patch management procedures when security weakness identified
  - Written risk management plan
  - Tighter standards for workforce clearance and termination
  - Annual security awareness training
  - Tighter contingency, backup and disaster recovery response and management
  - Specifications on physical security standards, including door access systems and surveillance
  - Monitoring system and ePHI activity in real time

Effect of New Administration

- Cybersecurity is a bipartisan issue, so these proposed rules may not be pulled down
- Can’t be finalized until March at the earliest
- Wait and see

Practical Issues

Reed + Claymon

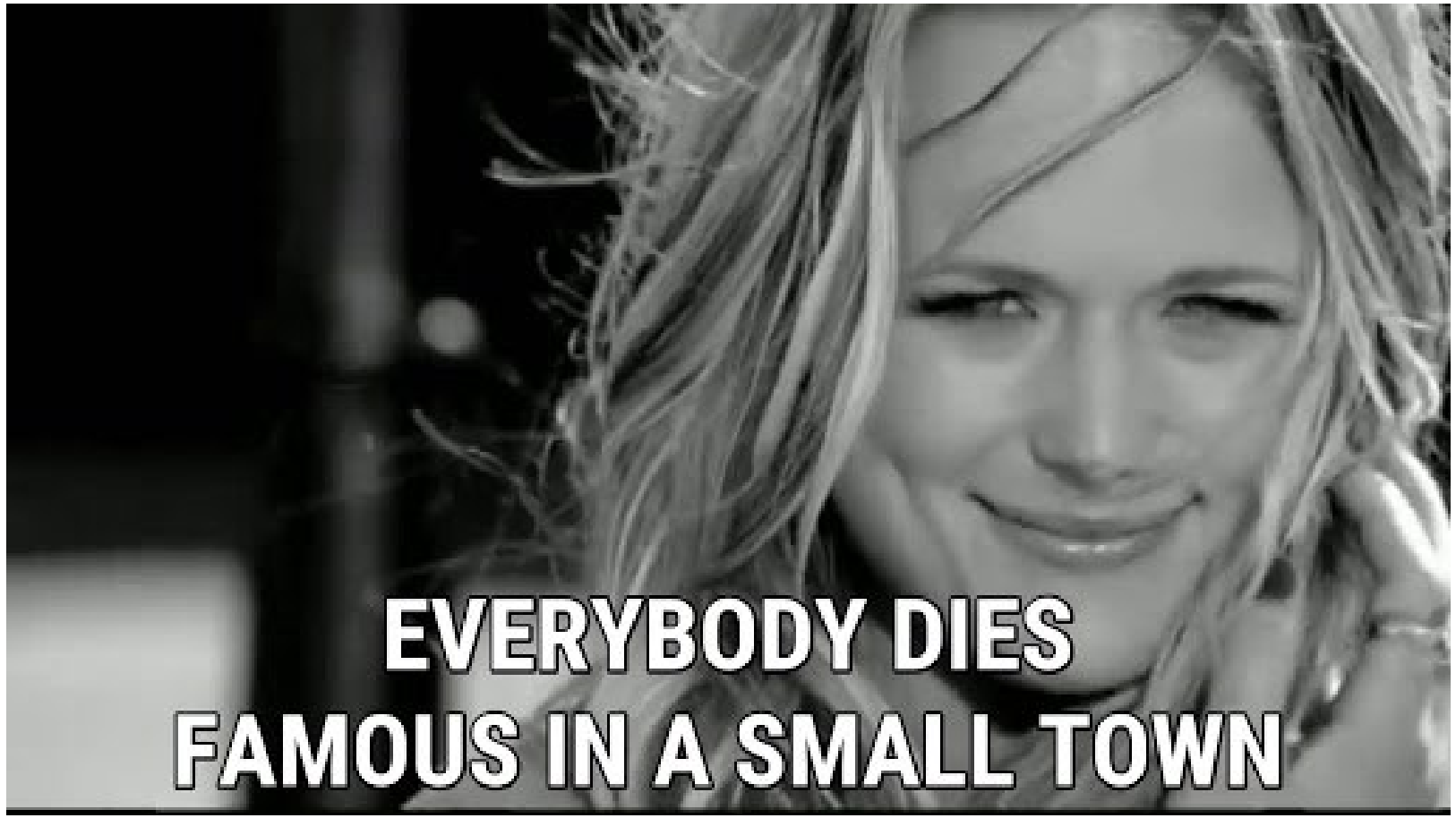
Friends, Family and Co-workers

- If patients of covered entity, have same rights and protections as any other patient
- Do not access PHI of friends, family or co-workers if you are not involved in providing health care to that individual
- Do not disclose PHI of friends, family or co-workers except as necessary to provide health care to that individual
  - What about health information that you become aware of outside of your role as health care provider?

Social Media

- Do not post anything about a patient on Facebook or any other website
  - It does not matter if you don't use the patient's name
- Don't take pictures that have patients in them (no photobombs; no picture of particularly gory wounds)
  - It does not matter if you can't see the patient's face

Reed + Claymon


EVERYBODY DIES
FAMOUS IN A SMALL TOWN

Tips to Secure Mobile Devices

- Encryption on mobile devices
  - iMessage is not HIPAA compliant
  - Only use HIPAA-compliant text messaging service specifically designed for healthcare professionals to communicate about patients
- Use a password or other user ID
- Wiping and/or remote disabling to erase data on mobile device if lost or stolen
- No file-sharing applications
- Firewall to block unauthorized access
- Security software to protect against viruses, spyware, malware, etc.

Tips to Secure Mobile Devices

- Keep security software up to date
- Research apps before downloading
- Maintain physical control of your mobile device – Know where it is at all times!
- Use adequate security if sending or receiving PHI over public Wi-Fi networks
- Delete all stored PHI before discarding mobile device

Reed Claymon

Can you have a confidential conversation with a patient where you can be overheard?

Reed + Claymon

YES – BUT …

- When required to have an efficient conversation
  - Nurses station OK
  - By phone at nurses station OK
  - In a joint treatment area OK
- But try for privacy
  - A nearby room
  - A lowered voice
  - A corner of the waiting area

When can information be disclosed for law enforcement purposes without patient authorization?

- As required by law
  - Example: Texas requires reporting of gunshot wounds to law enforcement
- In compliance with court orders or grand jury subpoenas
- To identify or locate suspect, material witness or missing person
- To report a crime on the premises
- To provide information about victim IF victim agrees

- If suspect death may have resulted from criminal conduct
- To report abuse or neglect of child, elderly or disabled
  - Domestic violence: Depends on state law

What information can be shared with friends/family of a patient?

Reed + Claymon

- Information that is directly relevant to the involvement of a spouse, family member, friend, or other person identified by a patient
  - Follow up care
  - Payment
- If patient does not object
- For hospitals, directory information

Examples of Disclosure to Friends/Family

Reed + Claymon

Reed + Claymon

Reed + Claymon

- Patient's doctor may discuss the drugs patient needs to take with patient's health aide who has come with patient to appointment

- Patient's nurse may tell patient that she is going to tell patient's brother how patient is doing, and then she may discuss patient's health status with patient's brother if patient did not say that she should not
  - BUT … Patient's nurse may not discuss patient's condition with patient's brother if patient tells her not to

Family Medical History

- The Privacy Rule does not limit an individual's ability to gather and share family medical history information
  - It does limit what a doctor can do with a family medical history
- A health care provider can disclose protected health information provided by a patient about the patient's family member to another provider, when such information is requested for the treatment of the individual patient

Incidental Uses and Disclosures

- Patient charts can be placed in plastic boxes outside an exam room
  - Turn them around to face the wall
- Patient sign-in sheets can be used and/or the patient's name can be called out in waiting rooms
- Messages for patients can be left at their homes, either on an answering machine or with a family member, to remind them of appointments or to inform them that a prescription is ready
- Appointment or prescription refill reminders can be mailed to patients' homes

Don’t Forget about State Law!

- Your state may have additional law or regulations governing privacy of health information.
- Any state law more restrictive than HIPAA is not pre-empted by HIPAA.

Jennifer Claymon
jclaymon@rcmhlaw.com
512.660.5965

Reed, Claymon, Meeker, Krienke
& Spurck, PLLC
901 S. Mopac, Suite 290
Austin, TX 78746
512.660.5960 main
512.660.5972 fax
reedclaymon.com

Questions?

Reed + Claymon