

HIPAA privacy: Learning the basics and what's new for 2026

Compliance Consulting

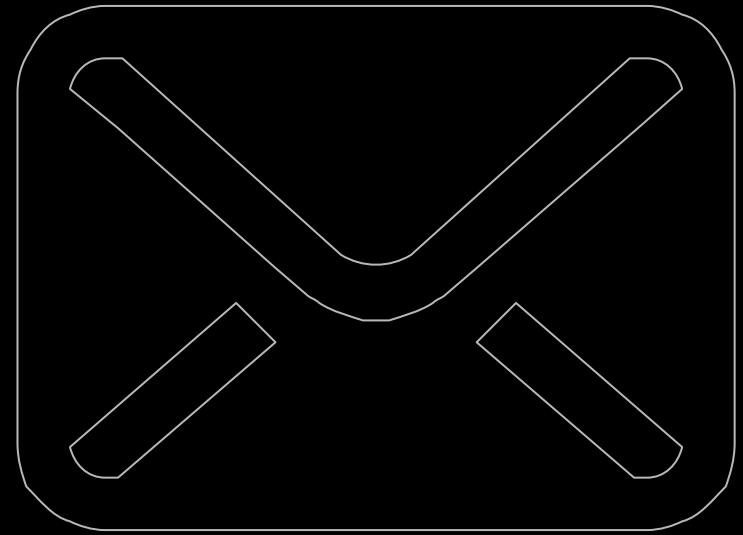


Ruhe Wadud, JD and Ethan McWilliams, MBA

April 16, 2026

Still waiting for your handout?

- Spam filters sometimes intercept messages sent from our group mail server. If you have not yet received the PowerPoint presentation for this webcast, please reach out to your Lockton account team.



Any questions?

- You can submit questions using the Q&A box on your computer screen.

We may attempt to answer some questions during the Q&A portion, near the conclusion of the presentation, if time permits.



Coming soon: our summer 2025 CLASS series

Costs, innovation, and emerging pharmacy strategies

2-3 p.m. CT, Thursday, May 14

Speakers: Rory Akers, JD and Matt Javris

Practical considerations for mergers & acquisitions

2-3 p.m. CT, Tuesday, Aug. 18

Speakers: Suzanne Bach, JD and Ethan McWilliams, MBA

Renewals for 2027: What to know and how to prepare

2-3 p.m. CT, Tuesday, June 9

Speakers: Mark Holloway, JD and Petra Wheaton, MBA

We'll email you the class schedule with registration links in the coming days.

HIPAA privacy: Learning the basics and what's new for 2026

Compliance Consulting



Ruhe Wadud, JD and Ethan McWilliams, MBA

April 16, 2026

Today's speakers



RUHE WADUD, JD
Vice President
Compliance Consulting



ETHAN MCWILLIAMS, MBA
Assistant Vice President
Compliance Consulting

AGENDA

HIPAA overview

Who is subject to the privacy and security rules?

What types of information are “protected?”

Rules regarding access, use and disclosure of PHI

Participant rights

Securing electronic PHI

Compliance strategies

What to do in the event of a breach

Enforcement



What's new about HIPAA in 2026?

Focus on “Part 2” confidentiality

- Requires covered entities to provide specific confidentiality to medical records of individuals with substance use disorders (SUD); specifically, records from federally assisted “Part 2” programs providing SUD care cannot be shared or disclosed without explicit patient consent.
- Revised Notice of Privacy Practice, Feb. 16, 2026
 - Should this include Part 2/SUD language as a default? Uncertain.

Reproductive health care disclosure protections face legal roadblock:

- Late 2024 HIPAA Privacy Rule protections related to *legal* reproductive health care were vacated on June 18, 2025.

Rising number of cyber threats sparks Health and Human Services scrutiny:

- Proposed cybersecurity rules issued January 2025 (more later)

HIPAA overview

HIPAA, the multiheaded monster

- Portability provisions to help people maintain coverage without losing coverage for preexisting conditions when changing jobs.
- Administrative simplification rules intended to standardize electronic healthcare transactions and reduce costs.
- Consumer protections intended to limit the ability of plan sponsors to discriminate against participants with health conditions outside of strict wellness program rules.
- Privacy and security standards intended to limit when covered entities can access, use and disclose protected health information (PHI) and mandate security safeguards for electronic PHI (ePHI).



HIPAA privacy and security compliance

- Covered entities (*for our purposes, the employer health plan*) may not access, use or disclose PHI, except as required or permitted under the privacy rules.
- Covered entities must implement reasonable safeguards to protect the confidentiality, integrity and availability of ePHI.



HIPAA privacy and security compliance

Health plans subject to HIPAA must implement:

- Privacy and security policies
- Privacy and security official(s)
- Privacy notice
- Risk analysis
- Firewalls
- Administrative procedures and forms
- Document retention and recordkeeping
- Business associate agreements
- And . . .



Certain individuals must receive HIPAA training

- Employees working on behalf of the health plan must receive training regarding these privacy and security rules (that's you!):
 - Training on HIPAA requirements
 - Training on the specific plan's policies and procedures for HIPAA compliance
- HIPAA recognizes that only certain employees of the plan sponsor help operate and administer the plan:
 - Benefits or human resources department
 - Internal legal counsel
 - Internal accounting
 - Facility and computer information staff

Who is subject to the privacy and security rules?

What entities must comply?

Covered entities include:

- Healthcare providers
- Healthcare clearinghouses
- Health plans
 - Includes insurance carriers issuing health insurance policies
 - Includes plans established by employers that provide virtually any health benefits

Covered entities generally DO NOT include employers:

- For HIPAA purposes, employer *plans* are viewed as separate entities outside the employer



Not all employer plans must comply

Subject to HIPAA

- Medical
- Vision
- Dental
- Healthcare flexible spending account
- EAP

Not subject to HIPAA

- Long-term & short-term disability
- Dependent care spending account
- Life insurance
- Accidental death & dismemberment
- Workers' compensation

NOTE: Narrow exemption for small, self-insured, self-administered programs with fewer than 50 eligible employees or retirees.

Fewer requirements for many insured plans

Self-insured plans, including HRAs and FSAs (but not HSAs) are subject to the full array of HIPAA requirements.

Insured plans: whether the full array of rules applies to an employer with fully insured plans depends on whether the sponsor can keep “hands off” the plan’s PHI.

- If “hands off” (doesn’t create or receive PHI), can rely on insurer for most compliance responsibilities
- Exceptions for permitted use of information:
 - Enrollment information
 - De-identified information and summary health information
 - Information disclosed under an authorization
- However, it is not always easy to do so for:
 - Wellness programs
 - Internal payment process
 - Handling requests for claims assistance

The plan's business associates

WHO?

The plan's business associates are third parties that provide services or perform functions for a covered entity that come into contact with PHI.

Examples include third-party administrators, benefits consultants and outside vendors.



HIPAA APPLIES

Privacy and security requirements apply **directly** to business associates. This means business associates are subject to all HIPAA requirements, including adopting policies and procedures, having a privacy officer, security officer, etc., and being subject to civil and criminal penalties.



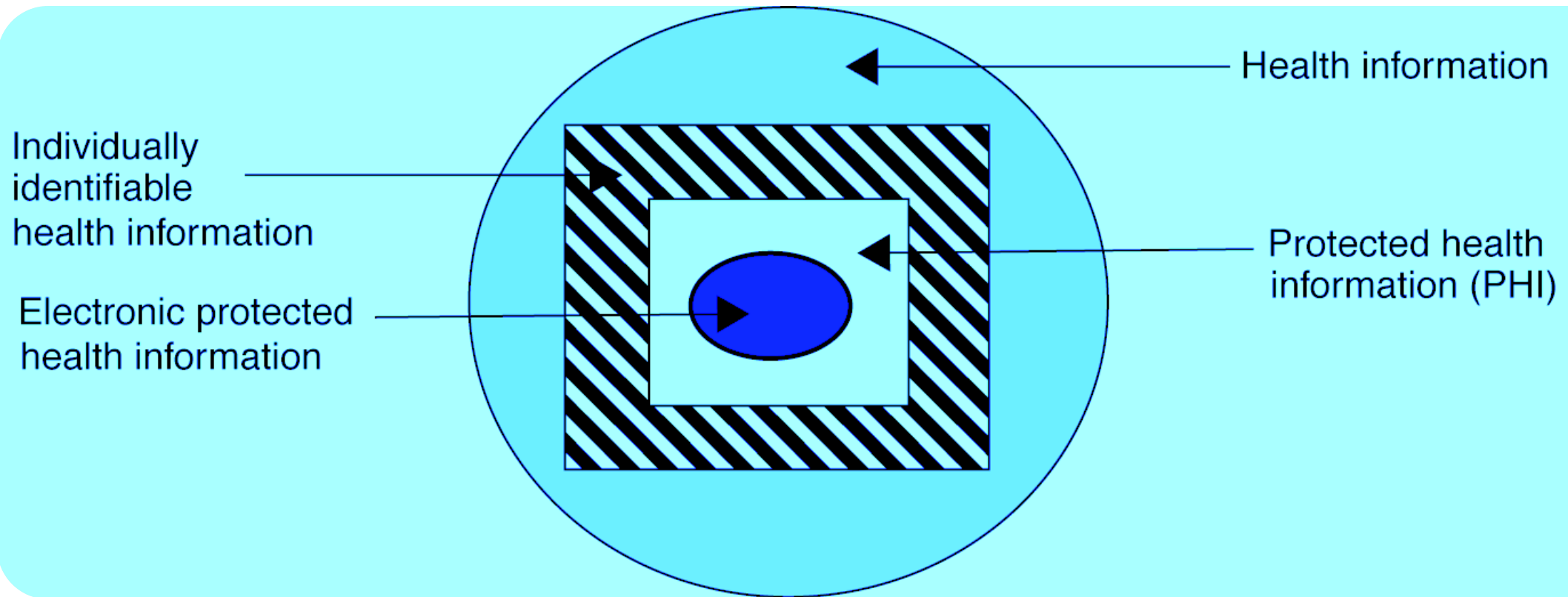
WRITTEN AGREEMENT

Covered entities must enter into "Business Associate Agreements" with business associates outlining HIPAA protections.



What types of information are
considered “protected?”

Types of information





Health information

Health Information is defined as information that relates to the:

- Individual's past, present or future physical or mental health **conditions**
- **Provision** of healthcare, and
- Past, present or future **payment** for healthcare.

Examples of health information

Medical plan
enrollment information

Medical plan claims
information

Diagnosis information

Medical plan coverage
information

Premium or
contribution
information

Individually identifiable health information

Health information could be individually identifiable if it contains:

- Names
- Geographic locators smaller than state
- Dates (birth, hire, ages over 89)
- Social Security numbers
- Telephone/fax numbers
- E-mail addresses
- Other unique identifiers:
 - Job title



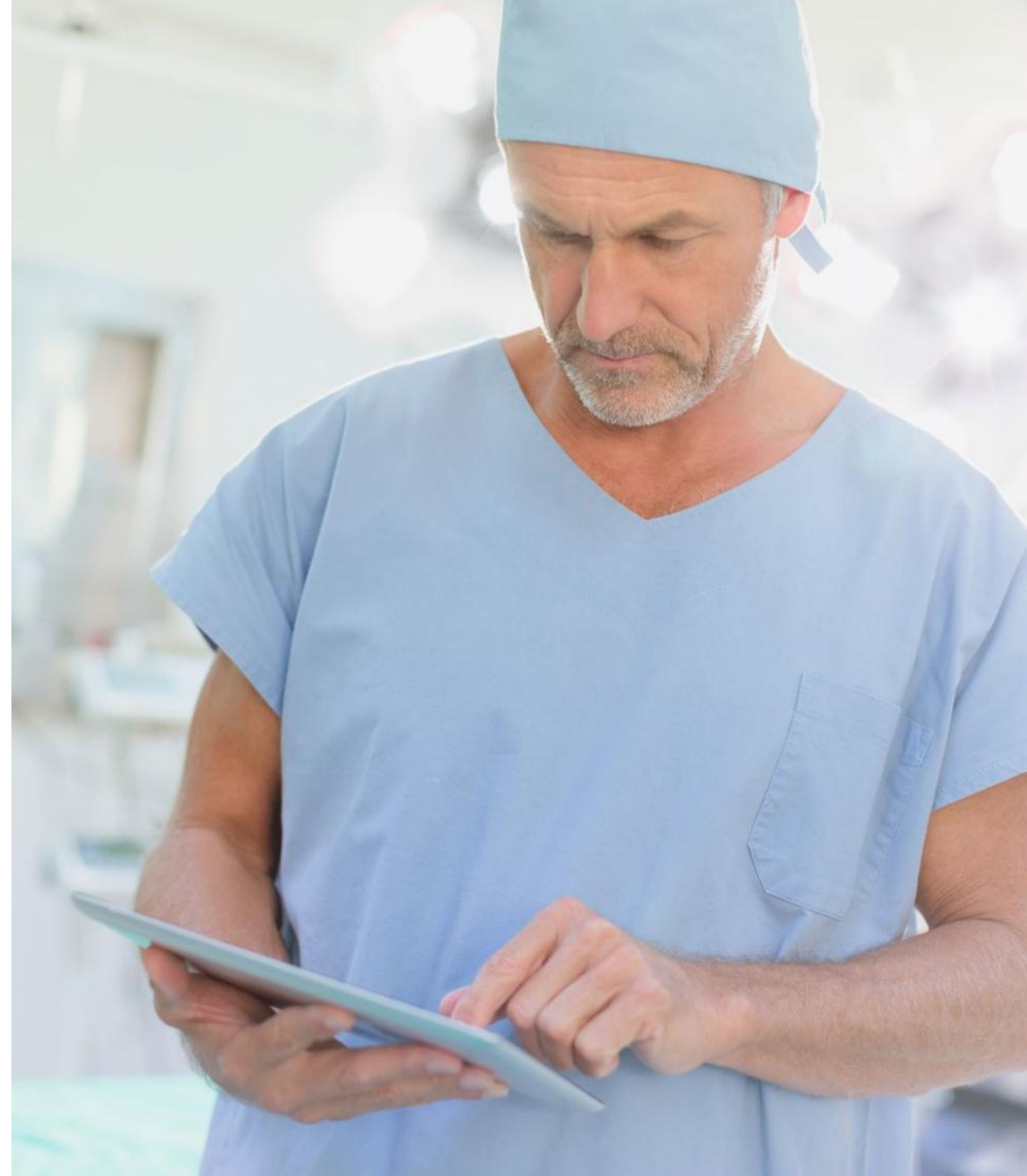
Protected health information

Protected health information is:

- Health information that is individually identifiable, and
- **Which is transmitted or maintained by a “covered entity.”**

Examples:

- Participant's Name + Enrollment + Transmission from plan = PHI
- Participant's SSN + claim submission + sent to health plan = PHI



Protected health information

- The following are not HIPAA-protected:
 - FMLA leave requests
 - Sick leave requests
 - Pre-employment screens
 - Workers' compensation claims
 - Return to work notes
 - STD or LTD applications or claims
 - Life insurance applications
 - Anecdotal information and gossip
- **BUT**, when it comes to securing any individualized health information, keep it all "top secret."
- Other laws such as the Americans with Disabilities Act require medical information to be held confidentially.

Rules regarding access, use and disclosure of PHI

Permitted uses and disclosures

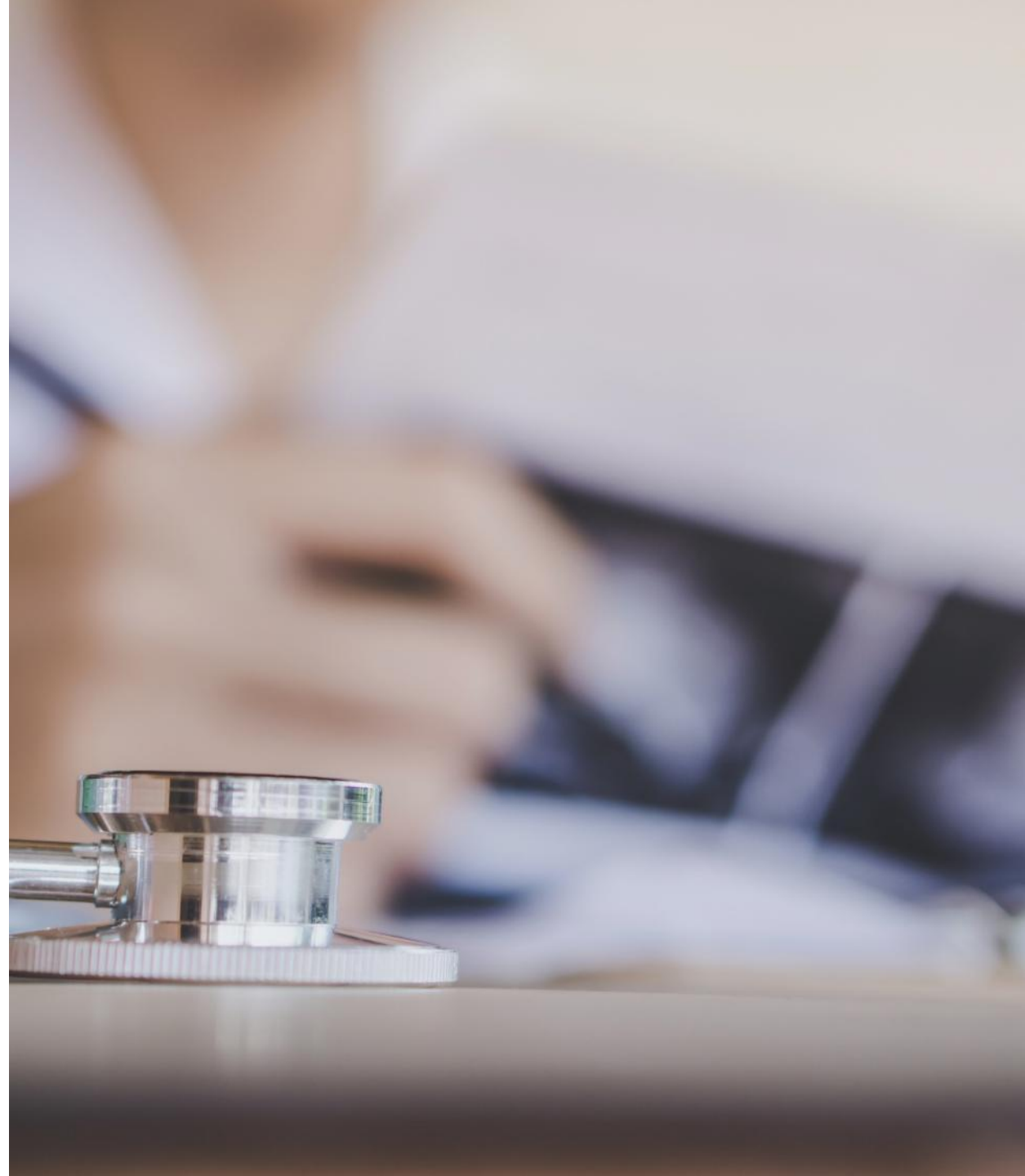
PHI may be used and disclosed by you for three purposes ("TPO"):

- **Treatment:** the provision, coordination or management of healthcare under the plan;
- **Payment:** activities to obtain or provide reimbursement for healthcare treatment under the plan; and
- **Healthcare operations:** activities relating to the plan's operations.

The good news: most activities involving the plan will be for TPO. But make sure the plan allows it and proper firewalls are in place.

Minimum necessary standard

- When uses, disclosures or requests of PHI are required, include only **the minimum necessary information** required to accomplish the intended purpose.
- Example: In determining whether the plan should cover a specific procedure for a participant, it would violate the minimum necessary standard to look at other participant claims to make that determination.



Permitted uses and disclosures

- Limited PHI involving a participant may be used and disclosed to the participant's family members and close friends.
- PHI may be used and disclosed if a participant has given written authorization.
- PHI may be used and disclosed in many special situations, including:
 - Workers' compensation programs (*if required to comply*)
 - Public safety
 - Legal process
 - Other unique times as included in the law

What not to do

Unless PHI is used or disclosed pursuant to:

- TPO,
- Written authorization, or
- Statutory exception...

... neither you nor the employer may use or disclose PHI obtained from the plan.

Neither you nor the employer may use any PHI from the plan for “employment-related” purposes:

- Disability claims processing
- FMLA leave processing
- Paid time off absence processing
- Employment actions



Participant rights

Participants' individual rights under HIPAA

- Right of **access** to PHI
- Right to **inspect** their PHI
- Right to **amend** PHI that is incorrect
- Right to an **accounting of disclosures** of their PHI made by the plan
- Right to request **restrictions** on disclosures of their PHI
- Right to request **alternate communications** of their PHI
- Right not to be subjected to **intimidation or retaliation** in connection with asserting their PHI rights

Rules have been proposed to further strengthen participant rights to access data.

The privacy notice

Requirements for privacy notice distribution:

- Must be distributed to participants at enrollment
- Must be reissued within 60 days of a material change
- Electronic delivery permitted if person consents in advance
- Privacy notice “reminder” is required every three years
- Best practice is to distribute full notice annually with open enrollment materials
- Upcoming model NPP change for fall 2026 open enrollment



Securing electronic PHI

How do the **privacy** and **security** rules interact?

The **privacy rules** govern how the plan may **use and disclose** PHI.



The **security rules** govern how PHI must be protected when it is in **electronic form**.

Electronic media

- Storage media (memory devices in computers, magnetic tape/disk, optical disk or digital memory card)
- Transmission media (internet, extranet, leased lines, dial-up lines)
- Electronic information systems



Three categories for safeguarding ePHI

Administrative

Security management process:

- Prevent, detect, contain and correct violations

Workforce security:

- Workforce members have appropriate access

Information access management:

- Authorize appropriate access

Security awareness and training

Security incident procedures

Contingency plan

Evaluation

Business associates

Physical

Facility access controls:

- Limit physical access

Workstation use:

- Specify proper functions, manner and physical attributes

Workstation security:

- Restrict access to workstations

Device and media controls:

- Monitor receipt, removal and movement

Technical

Access controls:

- Allow access only to authorized persons

Audit controls:

- Record and examine activity

Data integrity:

- Protect ePHI from improper alteration or destruction

Authentication:

- System of verification

Transmission security:

- Protect electronic communication

New! Electronic Data Security

- Numerous high-profile cyber attacks and data breaches involving ePHI
- [HHS "wall of shame"](#).
- Proposed rules would tighten data security rules, require speedier reporting of breaches and amendments to business associate agreements.
- Requirement of written documentation of policies, procedures, plans, and analyses.
- More details relating to the risk analysis covered entities must perform.
- Requirement for health plans to obtain, on an annual basis, written verifications from business associates that the business associates have deployed HIPAA technical safeguards.
- Business associates would also be expected to obtain such verification from their subcontractors.
- Will the Trump Administration allow the rule to be finalized?

Compliance strategies

Precautions – Ask these important questions:

Who?

Is the person authorized to use this information?

What?

Is the information protected (PHI); is the information received or being used the minimum necessary information?

Why?

Is the information being used for a permissible purpose such as TPO or is it being used for an impermissible purpose such as an employment reason?

Precautions – best practices

- Only discuss PHI obtained from the plan for plan purposes and take precautions against someone overhearing you.
- Do not use or disclose PHI to a third party without confirming that the proper agreements are in place.
- Do not use or disclose PHI to a third party without confirming that you are speaking with the proper person.

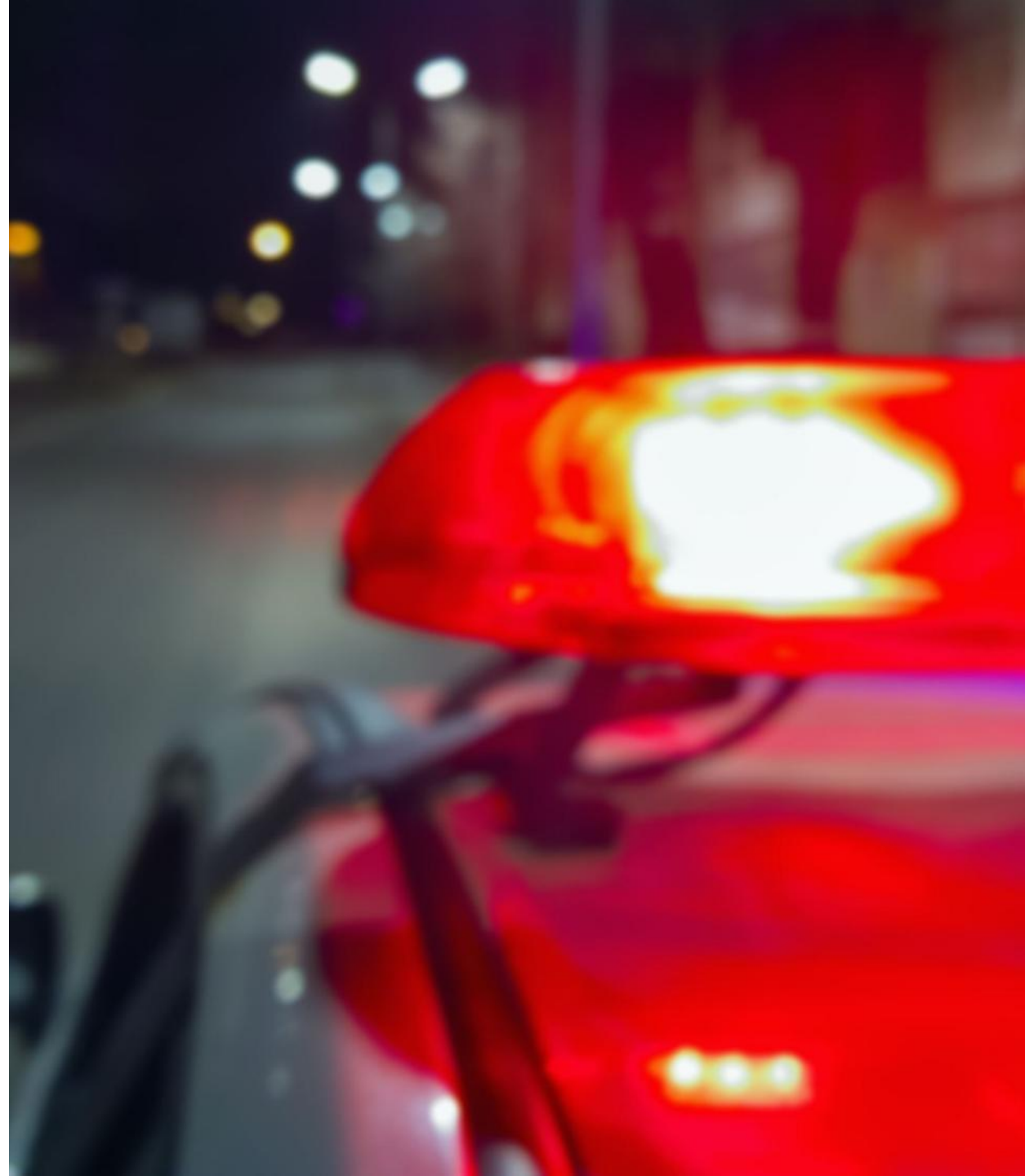


Precautions – securing physical surroundings

- Have storage cabinets locked or otherwise secured.
- Do not leave documents unattended.
- Use a screensaver and password to protect your desktop.
- Restrict faxes, copying, email, etc. to protect against disclosures.
- Restrict unauthorized personnel access to areas where PHI is used, including restricted office space.
- Destroy or return documents containing PHI when it is no longer needed (generally required to keep for six years).
- Encryption, encryption, encryption!
- Security officer must perform a risk analysis and address potential concerns.

Privacy and security officers

- If you have doubts, check with the plan's privacy or security officer.
- The officers are responsible for the development and implementation of the covered entity's privacy and security policies and procedures.



What to do in the event of a breach?

HIPAA breach notification requirements

There is a presumption that a breach occurred, but the health plan can analyze the situation to conclude whether a disclosure rose to the level of being a breach.

- Determining if a HIPAA breach occurred:
 - Was there PHI involved?
 - Was it “unsecured?”
 - Was there a use or disclosure of the PHI in violation of the HIPAA privacy rules?
 - Is there a low probability that the PHI has been compromised?
 - Can the risk be mitigated?
 - Is the breach otherwise forgiven (under the “incidental” exceptions)?



HIPAA breach notification requirements _____

- Plan must provide notice of a breach to the affected participant without unreasonable delay and within 60 days of discovery.
 - Notice requirements vary depending on the number affected and ability to find them.
- Exceptions:
 - Secured = Encrypted or destroyed per HHS requirements.
 - Encryption: Convert data to code requiring a password or key to decipher.
 - **Practical advice: encrypt, encrypt, encrypt!**
 - Other exceptions to breach notification requirements may apply, but don't rely on them.

Enforcement

Protected health information

- Does it really matter if confidential information is PHI?
- Plan participants cannot sue (yet) under HIPAA, and the HIPAA enforcement environment (via HHS) is rather benign vis-à-vis health plans.
- But enforcement is ramping up. Under the law, state attorneys general may sue
- Participants CAN sue to enforce terms of employer-sponsored plan, which must include privacy and security protections if the employer receives PHI or ePHI.
- Participants can file a complaint against the health plan that could lead to an investigation and fines.



Penalties

Financial penalties for noncompliance may include:

- \$145 per violation if person does not know of the violation (didn't know they broke the rules), up to \$73,011 per year for identical violations
- \$1,461 per violation due to reasonable cause, up to \$73,011 per year for identical violations
- \$14,602 per violation due to willful neglect, up to \$ 73,011 per year for identical violations
- \$ 73,011 per violation due to willful neglect where the entity did not correct the problem, up to \$2,190,294 per year for identical violations

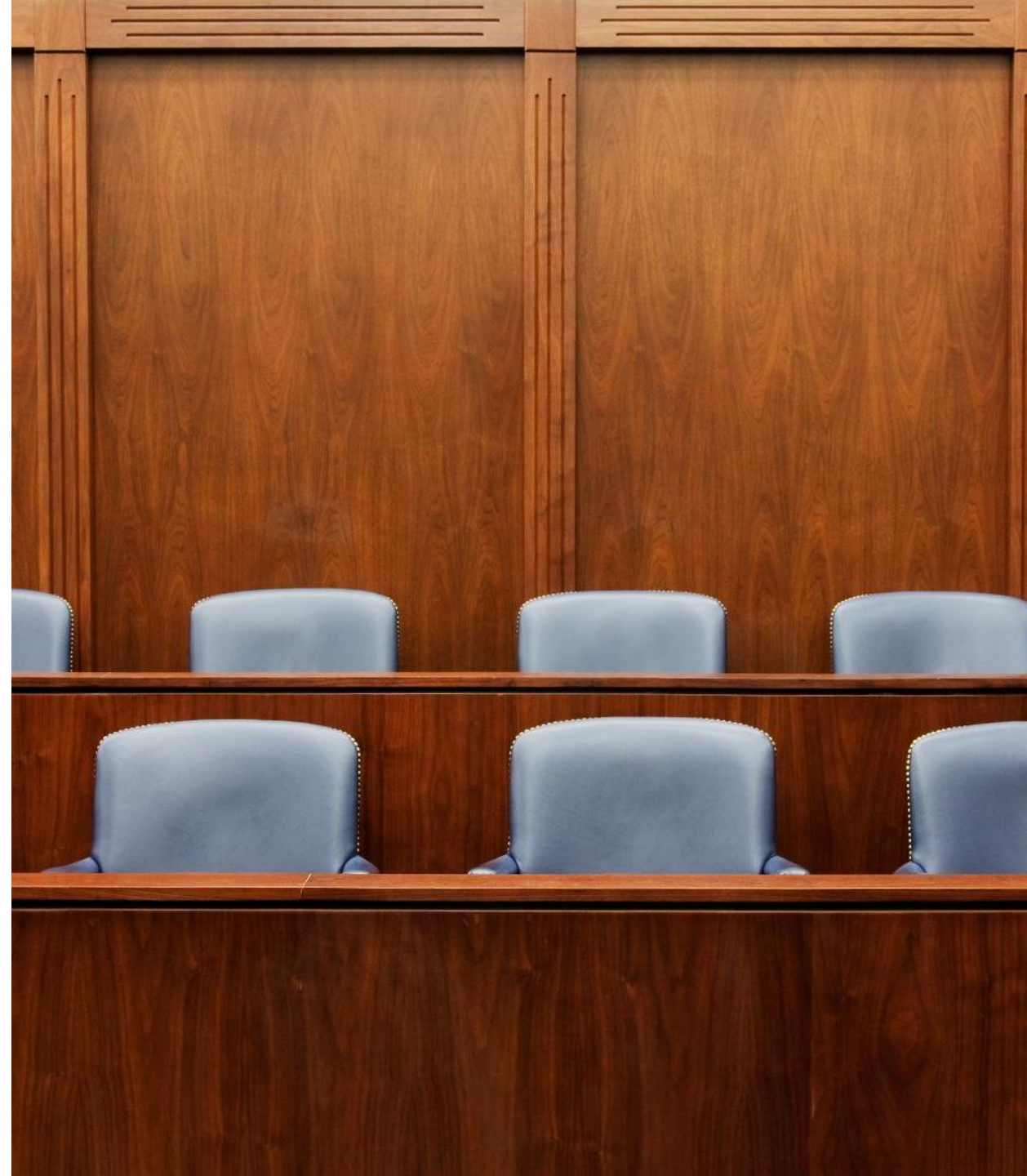


HIPAA Enforcement

- Since 2003 through late 2024, there have been 374,322 total complaints received!
- 99% resolved (most are resolved *before* investigation)
- Investigated complaints:
 - 67% result in corrective action
 - 33% - no violation found
- Almost \$150 million in settlements or penalties
- 77% of large breach reports due to hacking/IT incidents
- Top five issues:
 - Use and disclosure
 - Lack of safeguards
 - Lack of patient access
 - Lack of administrative safeguards of ePHI
 - Use and disclosure beyond the minimum necessary

Significant resolution agreements

- Medical center fined \$4.75 million for an employee stealing and selling patients' PHI over a six-month period.
- Local initiative health authority fined \$1.3 million for failure to secure member PHI.
- Health center LLC fined \$30,000 for impermissibly disclosing PHI of a patient when the entity posted a response to the patient's negative online review.



Questions?

**INDEPENDENCE
CHANGES
EVERYTHING.**



UNCOMMONLY INDEPENDENT