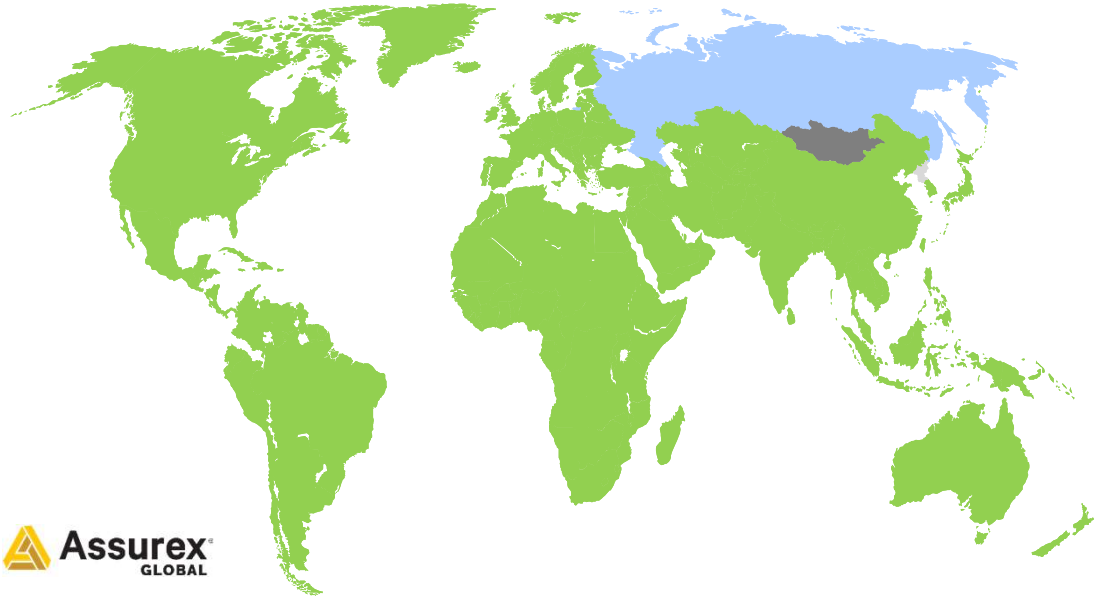
HIPAA Privacy & Security

Presented by Lumelight (formerly Benefit Comply)
July 2025

Thank you to the following Assurex Global Partners for sponsoring today's webinar

- C3 Risk & Insurance Services
- CCIG
- Christensen Group Insurance
- Collier Insurance
- Cottingham & Butler
- Cragin & Pike, Inc.
- The Daniel & Henry Co.
- Dean & Draper Insurance Agency
- Henderson Brothers, Inc.
- Houchens Insurance Group
- The IMA Financial Group
- INSURICA
- Kapnick Insurance Group
- The Mahoney Group
- The MJ Companies
- Oswald Companies
- The Partners Group
- R&R Insurance
- RCM&D
- Scott Insurance
- Starkweather & Shepley
- Sterling Seacrest Pritchard
- WA Group
- Watkins Insurance Group
- Wells Insurance



Assurex Global is an exclusive partnership of the most prominent independent insurance agents, brokers, and technical specialists in the world.

Assurex GLOBAL

Agenda

- HIPAA Background
- Privacy Rule
- Security Rule
- Breaches

Assurex GLOBAL

HIPAA Background

Assurex GLOBAL

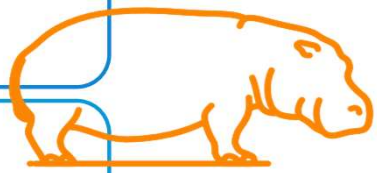
The Evolution of HIPAA

1996

Health Insurance Portability and Accountability Act ("HIPAA")
- Standardize healthcare transactions
- Help individuals to keep coverage

2003-2005

Privacy & Security Rules
- Protect confidentiality of PHI
- Create individual rights
- Protect health information in electronic format



2009-2013

HITECH & Omnibus Final Rule
- Increased oversight and enforcement
- Strengthened breach reporting
- Expansion to business associates

2024-2025

2024-2025

Recent Changes
- 2024 Privacy Rule (mostly vacated by *Purl v. HHS*)
- *Proposed* Security Rule Changes with more documentation requirements

Assurex GLOBAL

Who is Subject to HIPAA?

“Covered Entities”

Health Care Providers

Clearinghouses

Health Plans

“Business Associates”

Third parties that perform certain functions on behalf of a covered entity that involve the use or disclosure of PHI

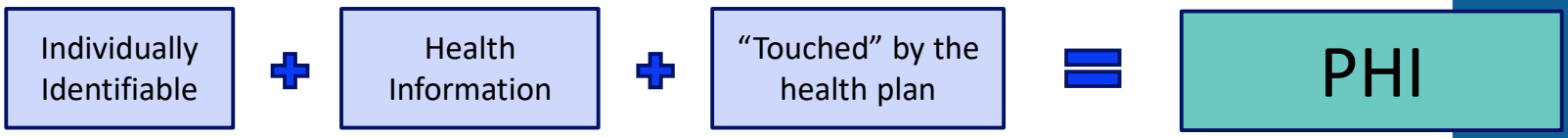
Ex. TPAs, brokers, consultants

Assurex GLOBAL

What Information Does HIPAA Protect?

Protected Health Information (PHI)

- Individually identifiable health information that has been created, received, or maintained by the health plan
- Includes name, address, DOB, SSN, etc. – not just treatment/diagnosis information



Not PHI:

- Health information gathered by plan sponsor as an employer (e.g., drug test results)
- Health information related to Worker's Compensation or FMLA claims
- Payroll information maintained by plan sponsor in its role as employ

Assurex GLOBAL

Employer-Sponsored Health Plans as Covered Entities

- The *health plan* is the Covered Entity, not the employer
- BUT as plan sponsor, an employer is responsible for their health plans' HIPAA compliance

Plans Subject to HIPAA
Medical; Dental; Vision; Prescription Drug; HRA; FSA; Retiree Health Plans; Expatriate Plans; Long-Term Care*; Wellness Program*; On-site Clinic*; EAP*

Plans Not Subject to HIPAA
Long-Term and Short-Term Disability; Accident; Life; Workers' Compensation; HSA*; Critical Illness*; Hospital Indemnity*; Fixed Indemnity*

Caution: Does **not** mean that this employee does not need to be protected

*HIPAA applicability can depend on actual benefits provided, but majority fall into the indicated categories

Assurex GLOBAL

Employer-Sponsored Health Plans as Covered Entities

- Plans are subject to HIPAA Privacy and Security Rules, but not Portability
  - Applicability depends on 1) funding and 2) access to PHI

Funding/Access to PHI	Subject to Privacy Rule?	Subject to Security Rule?
Self-funded Plans	Yes	Yes
"Hands-off" Fully-insured Plans*	Exempt but for prohibitions on retaliation and on waiver of rights	No clear exemption"
"Hands-on" Fully-insured Plans**	Yes	Yes

*Access only to summary health information and/or enrollment information
**Access to PHI beyond summary health information and/or enrollment information

- Summary Health Information – summarizes claims history, expenses, or type, and is stripped of all identifiers but for five-digit ZIP code
- Enrollment Information – High-level, nonclinical information; no claims or cost-sharing information or identifiable information

Assurex GLOBAL

Privacy Rule

Assurex GLOBAL

Permissible Uses/Disclosures of PHI

HIPAA restricts how CEs and BAs may use/disclose PHI

Treatment, Payment, & Health Care Operations

- Plan administration functions

To the Subject Individual or Their Personal Representative

- Parents of unemancipated minors
- NOT spouses or adult children
- Check documentation

Public Policy Purposes

- Health oversight activities; judicial/administrative proceedings; law enforcement; coroner or medical examiner; etc.
- 2024 Privacy Rule had complicated this category of permissible disclosure

Assurex GLOBAL

2024 Privacy Rule

- Introduced a prohibited use/disclosure of PHI potentially related to reproductive health care (RHC)
- Required HIPAA entities to request an attestation when PHI potentially related to RHC was requested for certain public policy reasons
  - Requestor attested that the PHI would not be used to impose liability for receiving, providing, or facilitating lawful RHC
- Mostly vacated by *Purl v. HHS*
  - Recent SCOTUS decision banning nationwide injunctions by judges does NOT apply here, so 2024 Privacy Rule is definitely vacated
  - "Mostly" - updates to Notice of Privacy Practices, comply by February 2026

Assurex GLOBAL

Permissible Uses and Disclosures of PHI

Any other use or disclosure of PHI will require the individual's authorization

- Opportunity to agree or object
  - Caller verification
- Written authorization
  - Check validity and scope

A valid authorization must have:

- Purpose
- Expiration date/event
- Description of PHI
- Identification of who can disclose and to whom
- Individual's dated signature

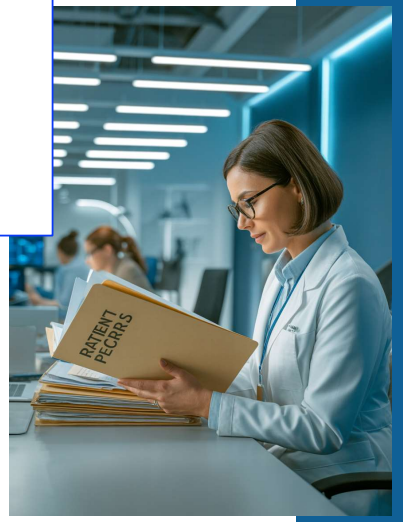
Assurex GLOBAL

Minimum Necessary

- Any use or disclosure of PHI must be limited to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request

- Common pitfalls:
  - Email strings
  - Unnecessary access to PHI
  - Oversharing with BAs
  - Misaddressed emails

Exceptions:
- Treatment
- To the individual
- Pursuant to an authorization
- To HHS
- Required by law



Assurex GLOBAL

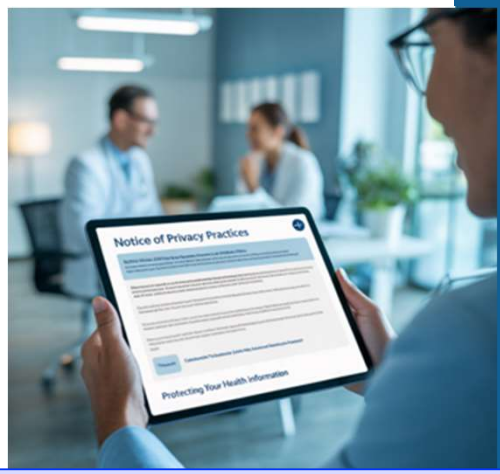
Impermissible Uses and Disclosures of PHI

- Employment-related actions or decisions
  - Hiring, firing, promoting, etc.
- Disclosure to employees not involved in plan administration
- Disclosure to adults who are not a personal representative
  - Spouses, adult children
- In connection with other benefits or employee plans
  - FMLA, disability, life

Assurex GLOBAL

Notice of Privacy Practices (NPP)

- **NPP Content Requirements**
  - Plan's uses and disclosures of PHI
  - Individual's rights with respect to their PHI
  - Plan's legal duties with respect to PHI
- **Distribution Requirements**
  - To new participants (in enrollment materials)
  - Within 60 days of any revision
  - To anyone who requests it
  - Reminder sent to participants every 3 years (or include in annual notice packet)



Remember:
- Updates to the NPP under the 2024 Privacy Rule, comply by Feb. 16, 2026
- New Model NPP expected

Assurex GLOBAL

Individual Rights

- Individuals have the right to:
  - ✓ Request access to PHI
  - ✓ Request amendment of PHI
  - ✓ Request an accounting of disclosures
    - Excludes disclosures for plan administration purposes
  - ✓ Request confidential communications of PHI
  - ✓ Request restrictions on use/disclosure of PHI
  - ✓ Make complaints
  - ✓ Receive a Notice of Privacy Practices

Covered Entities must respond to each type of request

Assurex GLOBAL

Administrative Requirements under the Privacy Rule

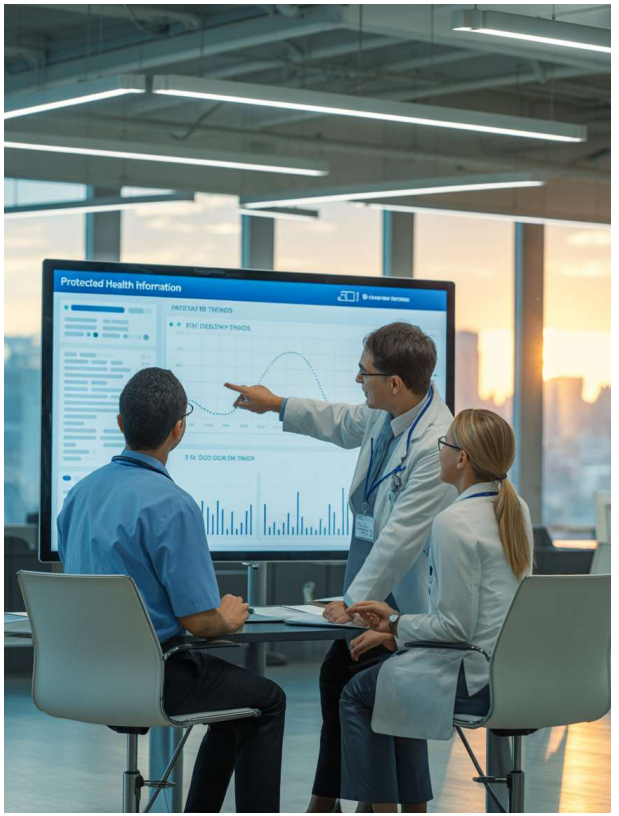
Covered Entities must establish requirements for safeguarding PHI in three categories:

- Physical safeguards
  - Restricting access to where PHI is stored, shredding paper PHI
- Technical safeguards
  - Role-based access controls, password protection
- Administrative safeguards
  - Identity verification, speaking quietly when discussing PHI

Assurex GLOBAL

Administrative Requirements under the Privacy Rule

- Appointment of a Privacy Official and Contact person
- Workforce training
- Prohibition on retaliation
- Prohibition on waiver of rights
- Written policies and procedures
- Business Associate Agreements



Assurex GLOBAL

Security Rule

Assurex GLOBAL

The Security Rule…

- Applies to electronic PHI (ePHI)
- Contains 22 standards, each with 0-4 implementation specifications

Safeguards/Requirements	Example Standard	Example Implementation Specification
Administrative Safeguards	Security Management Process	• Security Risk Analysis (Required)
Physical Safeguards	Facility Access Controls	• Facility Security Plan (Addressable)
Technical Safeguards	Access Controls	• Unique User Identification (Required)
Organizational, Policies/Procedures, Documentation Requirements	Group Health Plan Requirements	• Adequate Separation (Required)

- Flexible in implementation
  - Identifies what should be addressed, but does not specify exactly how
  - Consider: size, complexity, mission, purposes of ePHI created, maintained, sent, and received

Assurex GLOBAL

To Meet the Security Rule, In a Nutshell…

- Conduct a risk analysis
  - Helps to account for whereabouts of all ePHI, and identify security controls that are/should be applied

Review all ePHI

Identify threats, vulnerabilities, and risks

Review types of ePHI, location, access, audit log, etc.

Perform gap analysis

Develop risk management plan

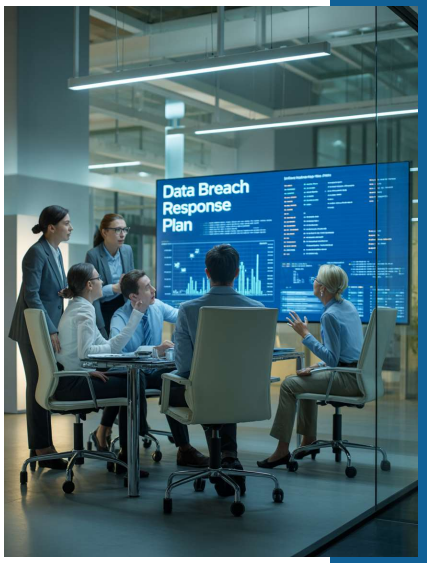
Implement security measures to reduce risk

Assurex GLOBAL

To Meet the Security Rule, In a Nutshell…

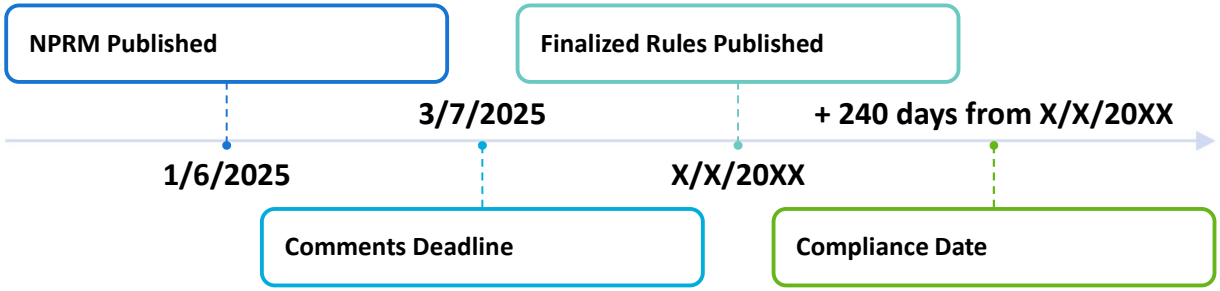
- Develop written security policies and procedures
  - Describes security controls that the risk analysis determined makes sense for the organization
- Appoint a Security Official
  - May delegate duties to others, but responsible for implementation of security controls
- Conduct security awareness training
- Periodically test/evaluate/refine security controls
- Coordinate Security Incident/Breach responses

Existing corporate security policies can and **should** be leveraged to meet and address Security Rule standards



Assurex GLOBAL

Proposed Changes to the Security Rule, In a Nutshell…



UNKNOWN: how or if the current administration will prioritize finalizing these rules.

Note: longer transition period allowed for necessary updates to Business Associate Agreements.

- Part of HHS' strategy to enhance cybersecurity in healthcare industry
- Elimination of "required" vs. "addressable" items
  - Addressable ≠ Optional
- 10 new definitions, 15 modified definitions
- New requirements as well as more specificity and rigidity around already-existing requirements:
  - Technology asset inventory and network map
  - Encryption for all ePHI

Assurex GLOBAL

So What Do We Do About These Proposed Changes?

Keep an eye out for finalized rules

Consider reviewing current security policies and procedures

- Proposed changes inform us on how enforcement may play out
- DOL Cybersecurity Best Practices

Assurex GLOBAL

Breaches

Assurex GLOBAL

What is a Breach?

*"…the acquisition, access, use, or disclosure of PHI in a manner not permitted under HIPAA which **compromises** the security or privacy of the PHI"*

Breach is assumed to have occurred unless a low probability of compromise can be demonstrated via a risk assessment based on four factors:

- Nature and extent of PHI involved, including types of identifiers and likelihood of re-identification
- Unauthorized person to whom unauthorized disclosure was made
- Whether PHI was actually accessed or viewed
- Extent to which risk to PHI has been mitigated

This assessment is part of the Privacy Officer's duties

Assurex GLOBAL

What is Not **a Breach?**

- Unintentional acquisition, access, or use by workforce member, if in good faith and within scope of authority, and no further use or disclosure
- Inadvertent disclosure to a colleague who is also authorized to access PHI, and no further use or disclosure
- Disclosure where there is a good faith belief that the unauthorized person was not reasonably able to retain the information

If There Has Been a Breach…

If breach affects fewer than 500 individuals:

- Affected individuals must be notified within 60 days of discovery of breach
- Include in annual log of breaches submitted to HHS within 60 days of end of calendar year

If breach affects 500 or more individuals:

- Affected individuals must be notified within 60 days of discovery of breach
- HHS must be notified within 60 days of discovery of breach
- Media outlets within the state/jurisdiction of affected individuals must be notified within 60 days of discovery of breach

Assurex GLOBAL

Breach Notification

- Sent to participants (or their representatives) whose information is reasonably believed to have been accessed, acquired, used or disclosed without authorized language
- Use plain language
- Include certain required information
  - Description of breach, dates, types of information involved
- Provide notice via:
  - First class mail
  - Email, if individual has agreed
  - If insufficient contact information, via telephone or media

Assurex GLOBAL

Business Associates and Breaches

- If a Business Associate gives notice of a breach, the Covered Entity should still go through its own process of determining if there is a breach

- Required notifications may be delegated to Business Associate as agreed upon – but Covered Entity still has ultimate responsibility

Assurex GLOBAL

Even if There isn't a Breach…

Mitigation

- Requesting disclosed PHI is destroyed
- Request that inappropriate recipient refrain from further disclosure
- Notification of individuals, media

Sanctions

- Any employee that violates HIPAA policies and procedure must be sanctioned
- May include retraining; warnings (verbal and/or written); suspension, demotion; termination
- Whistleblowers cannot be sanctioned

Complaints

- Complaints must be reviewed, investigated, and responded to

Assurex GLOBAL

Questions

Assurex GLOBAL

Webinar Wrap-Up

Thank you to the following Assurex Global Partners for sponsoring this event:

- C3 Risk & Insurance Services
- CCIG
- Christensen Group Insurance
- Collier Insurance
- Cottingham & Butler
- Cragin & Pike, Inc.
- The Daniel & Henry Co.
- Dean & Draper Insurance Agency
- Henderson Brothers, Inc.
- Houchens Insurance Group
- The IMA Financial Group
- INSURICA
- Kapnick Insurance Group
- The Mahoney Group
- The MJ Companies
- Oswald Companies
- The Partners Group
- R&R Insurance
- RCM&D
- Scott Insurance
- Starkweather & Shepley
- Sterling Seacrest Pritchard
- WA Group
- Watkins Insurance Group
- Wells Insurance

A link to the recording of today's session will be available early next week from the Assurex Global Partner Firm who invited you to today's event.

Assurex GLOBAL

Assurex Global in Numbers

26K+ Employees

100+ Partner Firms

$46B Annual Premium

$4.9B Annual Revenue

730+ Partner Offices

175 Countries