Arthur J. Gallagher & Co.
BUSINESS WITHOUT BARRIERS™

Don’t Be the Next Headline: HIPAA Basics

Sally Wineman, JD
Area Senior Vice President, Compliance Counsel

HIPAA

Privacy

Security

Risk Analysis

HIPAA

Privacy

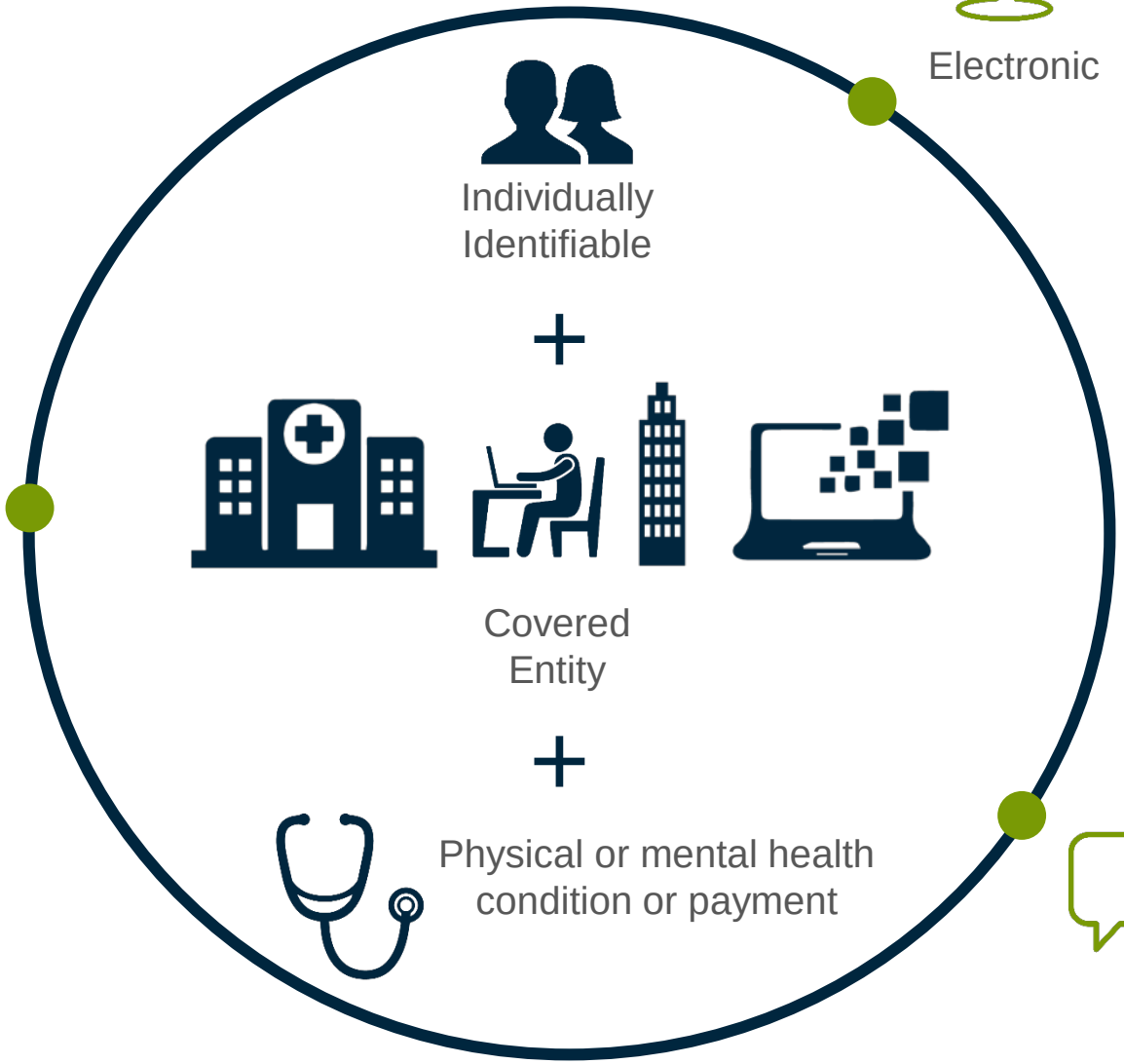
Security

Risk Analysis

Breach

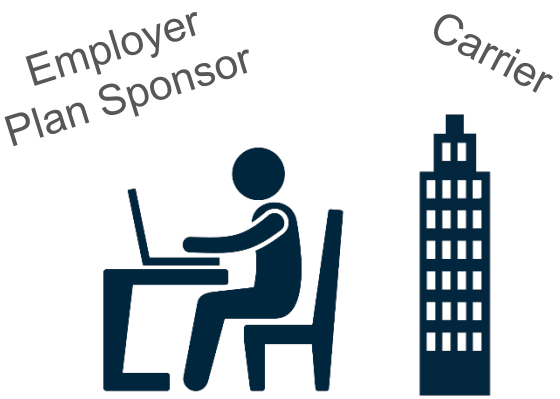
PHI

PHI



Parties

Hospital/
Provider



Health
Plan

Healthcare
Clearinghouse

Business Associates

(Lawyers, Brokers,
Accountants, TPAs, etc.)

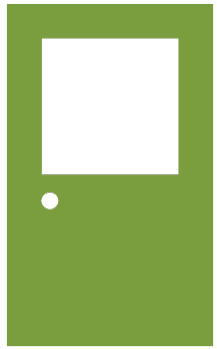
Privacy: Basic Requirements

- Protect confidentiality of PHI
- Use or disclose PHI only
  - Permitted by HIPAA or
  - As required by law
  - Minimum necessary standard applies
- Obtain written permission from patient for any other use or disclosure
- May use de-identified information

Business Associate Agreements

- Business associates
  - Required to comply with HIPAA – including security standards
  - Report breaches of PHI
  - Subcontractors
  - Comply with Privacy Rule where applicable
- Subcontractors also need Business Associate Agreements

Plan's Obligations



- HIPAA privacy policies & procedures
- Assign a privacy officer
- Privacy training
- Plan sponsor certification
- Plan document describes how the plan will use PHI and who (titles) will have access
- Permit individuals to access their own PHI
- Create and distribute HIPAA privacy notices
  - Initially
  - When change in policy or procedures
  - Notice of availability every 3 years

Action Items

HIPAA Privacy Action Items
☐ Inventory your PHI
☐ Determine who is a BA. If new, enter into a BAA
☐ Check all current BAAs
☐ Determine subcontractor BAs (if any)
☐ Determine your agents (if any)
☐ Update and issue revised Notice of Privacy Practices (if needed)
☐ Review and modify policies and procedures
☐ Update and conduct training

Security: Basic Requirements

- Applies to health plans
- Three types of security standards required
  - Administrative: Security management process
  - Physical: Device and media controls
  - Technical: Access control

Security: Basic Requirements

- Must satisfy if appropriate
  - If not, may use an alternative
- Addressable implementation specifications
  - Administrative: Security reminders
  - Physical: Data backup
  - Technical: Automatic logoff
- Be prepared to defend decisions!

Action Items

HIPAA Security Action Items

- ☐ Inventory ePHI
- ☐ Review and update as needed:
  - Risk assessment
  - Policies and procedures
  - Training
  - BAAs
- ☐ Document, document, document

Breach

- Breach is presumed
  - Burden on covered entity to establish low probability that unsecured PHI was compromised
- If unsecured PHI is breached, notification must be provided to:
  - Individuals affected
  - OCR
  - Media *(in some cases)*
- Covered entity must conduct a risk assessment and document the results

Breach Notification

Information “unsecured”? — NO → No breach. Documentation recommended.

YES

Violation of HIPAA Privacy rule? — NO → No breach. Documentation recommended.

YES

Meets risk of harm threshold? — NO → No breach, but document.

YES

Do any “breach” exceptions apply? — YES → No breach, but document.

NO

Provide notice

- Affected individual if acting as covered entity under HIPAA
- To covered entity if business associate acting as agent of covered entity

Make HHS notification and any required media notification

Breach Notification

Individuals	• All affected individuals: “Immediately”*
HHS	• 1-499: Annual log using OCR’s online portal, 60 days after end of year • 500 or more: “Immediately”*
Media	• 500 or more in a single jurisdiction: “Immediately”*

** No later than 60 days after discovery*

Action Items

HIPAA Security Action Items

- ☐ Consider (or re-consider) using encryption for ePHI
- ☐ Update training and retrain workforce members:
  - Employees
  - Interns
  - Volunteers
- ☐ Review and update notification procedures
- ☐ Address breach notification in BAA

Penalties & Fines

No knowledge

Reasonable cause

Willful neglect

HHS Enforcement

"OCR Announces Initiative to More Widely Investigate Breaches Affecting Fewer than 500 Individuals"

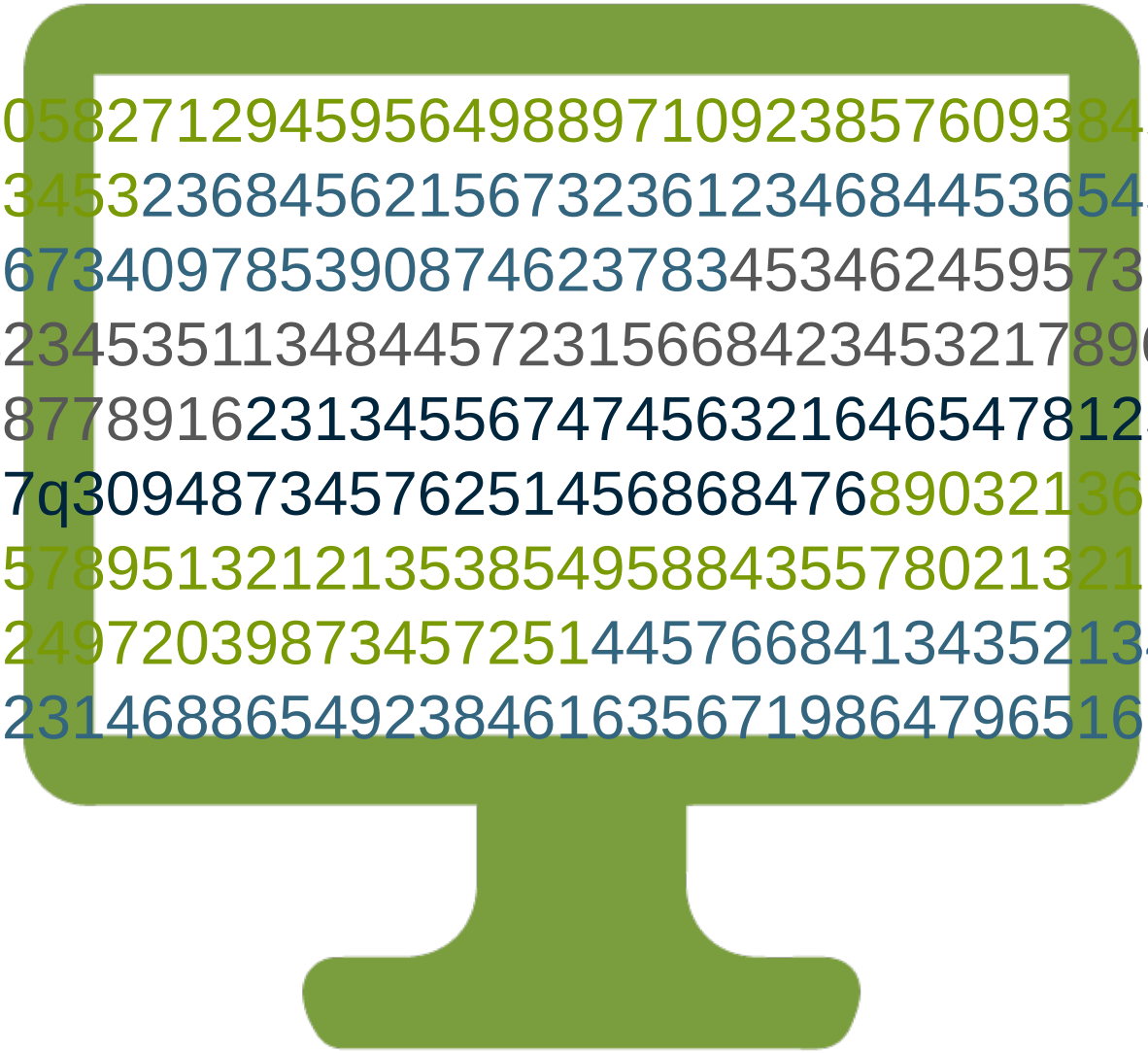
"Business Associate's Failure to Safeguard Nursing Home Residents' PHI Leads to $650,000 HIPAA Settlement"

"Widespread HIPAA vulnerabilities result in $2.7 million settlement with Oregon Health & Sciences University"

"Multiple alleged HIPAA violations result in $2.75 million settlement with University of Mississippi Medical Center"

Health Plan Identifiers

DELAYED!!!



GBS HIPAA Solutions

- Comprehensive, customized, and flexible proprietary process
- HIPAA Privacy and/or Security
  - Policies and procedures with corresponding forms
  - On-site training
  - Recorded webinar
- Security Risk Analysis with a written report

Arthur J. Gallagher & Co.
BUSINESS WITHOUT BARRIERS™

HIPAA Privacy and Security Services

A customized solution for your HIPAA Privacy and Security obligations.

Why comply with HIPAA Privacy and Security requirements?

The Department of Health and Human Services has the authority to impose substantial penalties upon employers who do not comply with HIPAA Privacy and Security obligations. Penalties in recent years have reached as high as $3.5 million.

What are an employer's key HIPAA Privacy and Security obligations?

Under HIPAA, all employer-sponsored self-insured health plans and fully insured health plans, receiving or maintaining more than summary health information or enrollment/disenrollment information, must not only implement written Privacy and Security policies and procedures, but also, train all members of the health plan's workforce on those policies and procedures. Moreover, the Security policies and procedures must be based on a written Risk Analysis.

How does Arthur J. Gallagher & Co. help?

The Benefits & HR Consulting division of Arthur J. Gallagher & Co. has developed a comprehensive, customized, and yet flexible proprietary process that is designed to provide employers with the right solution for their HIPAA needs. This includes:

- Customized written Privacy policies and procedures with corresponding forms, customized training via recorded webinar and a session of live on-site training for as many workforce members as the employer wishes to invite.
- Customized written Security policies and procedures with corresponding forms, customized training via recorded webinar and a session of live on-site training.
- Security Risk Analysis resulting in a written report for the employer to consider. The written report can also be used by the employer to establish compliance with the requirement in the event of an audit

The complete suite of services is available for $25,000—however, Gallagher can work with you to craft a specific, scalable solution to meet your unique needs.

Consulting and insurance brokerage services to be provided by Gallagher Benefit Services, Inc. and/or its affiliate Gallagher Benefit Services (Canada) Group Inc. Gallagher Benefit Services, Inc. a non-investment firm and subsidiary of Arthur J. Gallagher & Co., is a licensed insurance agency that does business in California as "Gallagher Benefit Services of California Insurance Services" and in Massachusetts as "Gallagher Benefit Insurance Services." Securities and Investment Advisory Services may be offered through NFP Adviser Services, LLC, Member FINRA/SIPC. NFP Adviser Services, LLC is not affiliated with Arthur J. Gallagher & Co. or Gallagher Benefit Services, Inc. Neither Arthur J. Gallagher & Co., NFP Adviser Services, LLC or their affiliates provide accounting, legal, or tax advice.

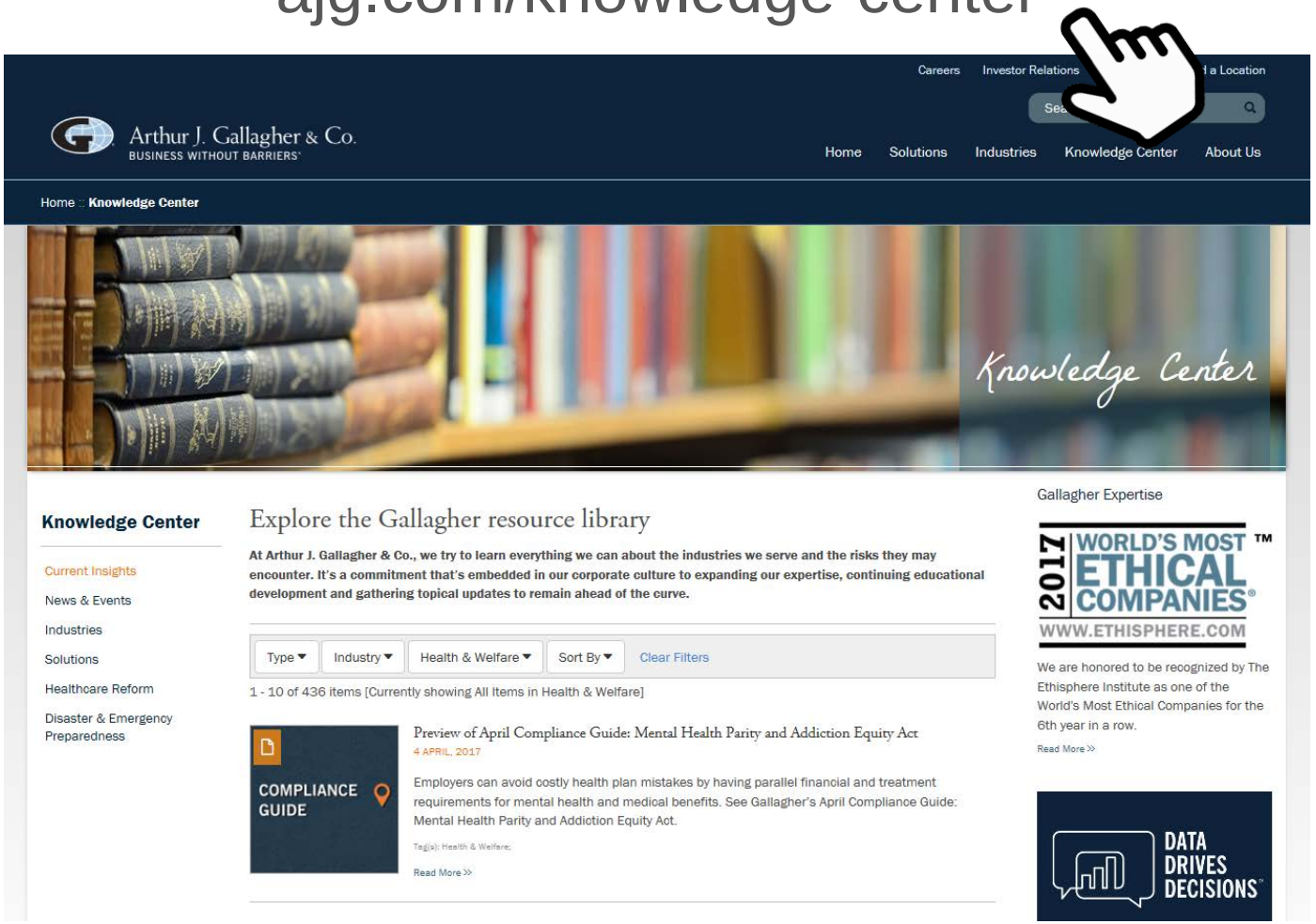
How do you start?

The process is easy and straightforward. If you are interested in exploring this customized and comprehensive solution to your HIPAA obligations, please contact your Gallagher consultant. As an alternative, you can submit your inquiries by sending an email to: gbs.HIPAAsolutions@ajg.com. We can explain each component of the solution and help you craft the exact offering that meets your specific needs.

1GBS29258A

Resources

ajg.com/knowledge-center



THANK YOU!