The mission of the Aging and Disability Business Institute (Business Institute) is to successfully build and strengthen partnerships between community-based organizations (CBOs) and the health care system so older adults and people with disabilities will have access to services and supports that will enable them to live with dignity and independence in their homes and communities as long as possible.

www.n4a.org/businessinstitute
PARTNERS AND FUNDERS

Partners:
• National Association of Area Agencies on Aging
• Independent Living Research Utilization/National Center for Aging and Disability
• American Society on Aging
• Partners in Care Foundation
• Elder Services of the Merrimack Valley/Healthy Living Center of Excellence

Funders:
• Administration for Community Living
• The John A. Hartford Foundation
• The SCAN Foundation
• The Gary and Mary West Foundation
• The Colorado Health Foundation
• The Marin Community Foundation

HIPAA & HITECH COMPLIANCE
FOR CBO & HEALTH CARE
PARTNERSHIPS:
THE MECHANICS OF
COMPLIANCE

PRESENTER: SHARON R. WILLIAMS, CEO
WILLIAMS JAXON CONSULTING, LLC

PART OF THE AGING AND DISABILITY
BUSINESS INSTITUTE SERIES - A
COLLABORATION OF N4A AND ASA
HIPAA MECHANICS: LEARNING OBJECTIVES

- Webinar Participants will:
  - Understand key components of the HIPAA & HITECH Act Privacy/Security Rules
  - Identify roles of Covered Entities & Business Associates
  - Understand the implications for CBOs as Business Associates
  - Review key mechanics of privacy/security compliance programming

Heavily regulated industry
  - Myriad federal/state regulations
  - HIPAA is by far among the most arduous federal regulations
  - States specific privacy regulations
  - Compliance implications
  - Ideal partners for the industry are knowledgeable, supportive & mitigate risk
LEGISLATION DU JOUR

- Health Insurance Portability and Accountability Act (HIPAA)
- Health Information Technology for Economic and Clinical Health Act (HITECH Act)
HIPAA IN THE BEGINNING...

- Pub.L. **104-191**, 110, aka Kennedy-Kassenbaum Act (Ted Kennedy/Nancy Kassenbaum; co sponsors)
- Enacted by Congress August 21, 1996 and signed by President Bill Clinton
- **Title I** protects employer sponsored health insurance coverage when people change or lose their jobs

HIPAA 2.0

**Title II:** enacted 2003
- aka the Administrative Simplification Rule:
  - Privacy
  - Security
  - Transaction
  - Unique National Identifier (NPI)
  - Fraud and Abuse
Title II

- Privacy Rule
  - Protect individual rights re: use, disclosure and access to health care data

- Security Rule
  - Establish safeguards for the protection of individual health care data
PRIVACY RULE

- Defines: Individually Identifiable Health Information (Protected Health Information PHI)
- Identifies: Roles & Responsibilities of Covered Entities & Business Associates
- Addresses: Allowable data disclosures for health care operations (TPO)
- Establishes: Penalties for violations under the DHHS Office of Civil Rights

‘A covered entity or business associate may not use or disclose protected health information, except as permitted or required by [the HIPAA Privacy Rule] or by subpart C of part 160 of this subchapter...’
**Protected Health Information: IIHI**

- Individually Identifiable Health Information, held or maintained by a Covered Entity or its Business Associates acting for the Covered Entity, that is transmitted or maintained in any form or medium.
- Including identifiable demographic and other information relating to the past, present, or future physical or mental health or condition of an individual, or the provision or payment of health care to an individual that is created or received by a health care provider.

<table>
<thead>
<tr>
<th>Identity Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Driver’s License #</td>
</tr>
<tr>
<td>Social Security#</td>
</tr>
<tr>
<td>Medical Record #</td>
</tr>
<tr>
<td>Phone #</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Personal Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
</tr>
<tr>
<td>Address (including zip code, city/state)</td>
</tr>
<tr>
<td>Email address</td>
</tr>
<tr>
<td>Dates of birth, death, discharge</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Medical Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Photographs</td>
</tr>
<tr>
<td>Biometric identifiers, including voice/finger prints</td>
</tr>
<tr>
<td>Genetic information</td>
</tr>
<tr>
<td>Distinguishing characteristics...shoe size??!!</td>
</tr>
</tbody>
</table>
ALLOWABLE USES & DISCLOSURE OF PHI

- Shared between health care entities (other Covered Entities and Business Associates) for Treatment, Payment and health care Operations
- As de-identified for public health, research purposes
- As required for law enforcement

COVERED ENTITIES & BUSINESS ASSOCIATES

Covered Entities (CE)
- Responsible for compliance with HIPAA/HITECH Act requirements
- Must identify Business Associates and execute Business Associate Agreements
- Health plans, Insurers, HMOs, Providers, Employer sponsored health care organizations, government sponsored health care programs
- Must issue Notice of Privacy Practices (NOPP)

Business Associates (BA)
- Responsible for meeting HIPAA/HITECH Act standards per execution of contract/BAA with a Covered Entity
- Business Associate
- Performs a function/service on behalf of a Covered Entity involving use/disclosure of PHI
- Must report privacy/security breaches to Covered Entity
BAA
- Issued by the Covered Entity
- Must be accompanied by a Contract for services
- Binds BA to comply with CE’s privacy/security rules and HIPAA rules

Which is why you must have a strong HIPAA Compliance Program

BAA:
- Establishes the permitted and required uses and disclosures of protected health information by the Business Associate.
- May permit the Business Associate to use and disclose protected health information for the proper management and administration per the CE contract.
- May not authorize the Business Associate to use or further disclose the information that would violate the requirements of the HIPAA Privacy Rule
Limits unnecessary or inappropriate access to, use and disclosure of PHI

Create policies & procedures to ensure compliance Minimum Necessary standards, such as:

- Identify the persons or classes of persons within the organization who need access to the PHI to carry out their job duties
- Identify the categories or types of PHI needed, and conditions required to provide access
Security Rule

- Operationalizes protections in Privacy Rule
- Rule requires affected entities to provide Administrative, Technical and Physical Safeguards for protecting PHI
- Designate a Security Officer

Security Rule

- The Rule identifies security standards and established Required and Addressable implementation specifications:
  - **Required** specifications must be adopted and administered as dictated by the Rule
  - **Addressable** specifications allow for flexibility in implementing/administering Rule specifications
Administrative Safeguards

- Administrative Safeguards
  - Designate a Privacy Officer
  - Adopt written privacy procedures that address:
    - Restricted access to ePHI
    - Establish internal audits
    - Document instructions for security breaches
    - Document sanctions
  - Establish comprehensive/ongoing training
  - Establish role based access standards for employees
  - Vendors compliance
  - Disaster Recovery Planning

Technical Safeguards

- Access Control
  - Information Systems ePHI access security

- Audit Controls
  - Record and examine access and other activity in Information Systems
  - Risk analysis and risk management programs

- Integrity Controls
  - Alteration/Destruction of ePHI

- Transmission Security
  - Technical security measures to restrict unauthorized access to electronically transmitted PHI
  - Encryption
  - Authentication
Facility Access and Control
- Limit physical access to facilities, especially work areas where ePHI is housed.

Workstation and Device Security
- Policies and procedures specify proper use of and access to workstations and electronic media where ePHI is housed.
- Policies and procedures addressing the transfer, removal, disposal, and re-use of electronic media, to ensure appropriate protection of ePHI.

HITECH ACT
**HITECH ACT**

- Subsection of American Recovery and Reinvestment Act, enacted 2009; compliance required 2013
- Strengthens Privacy Rule protections:
  - Extends Privacy Rule compliance requirements & penalties to BAs
  - Expands standards for reporting unintentional disclosures

**REPORTING BREACHES**

- Establishes new security breach notice requirements:
  - Requires that CEs/BAs that access, maintain, unsecured PHI and discover a breach of this information must notify each individual whose health information has been, or is reasonably believed to have been, accessed, acquired, or disclosed as a result of the breach.
  - BAs must to provide notice of data breaches to the CE
  - BAs/CEs must identify each individual whose unsecured protected health information was illegally accessed, acquired, or disclosed.
HITECH ACT: DESTRUCTION OF PHI

- **Paper, film, or other hard copy media** must be shredded or destroyed so that the PHI cannot be read and/or cannot be reconstructed.
- **Electronic media** must be cleared, purged, or destroyed consistent with NIST Special Publication 800-88, *Guidelines for Media Sanitization* so that the PHI cannot be retrieved.


HIPAA ENFORCEMENT
HIPAA ENFORCEMENT

US Department of Health and Human Services and the Office of Civil Rights
- Oversight/Monitoring/Reporting
- Review/Investigate complaints
- Levy sanctions

MOST COMMON CITATIONS*

- Misuse and disclosures of PHI
- Failure to establish adequate protections of health information
- Patient unable to access their health information
- Using or disclosing more than the minimum necessary protected health information
- Failure to establish safeguards of electronic protected health information

* HHS Ofc of Civil Rights
### HIPAA ENFORCEMENT: CIVIL

<table>
<thead>
<tr>
<th>Type of Violation</th>
<th>CIVIL Penalty (minimum)</th>
<th>CIVIL Penalty (maximum)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Individual unaware (and by reasonable diligence wouldn’t have known) that they violated HIPAA</td>
<td>$100 per violation, with an annual maximum of $25,000 for repeat violations</td>
<td>$50,000 per violation, with an annual maximum of $1.5 million</td>
</tr>
<tr>
<td>Not willful neglect</td>
<td>$1,000 per violation, with an annual maximum of $100,000 for repeat violations</td>
<td>$50,000 per violation, with an annual maximum of $1.5 million</td>
</tr>
<tr>
<td>Willful neglect and violation is corrected within the required time period</td>
<td>$10,000 per violation, with an annual maximum of $250,000 for repeat violations</td>
<td>$50,000 per violation, with an annual maximum of $1.5 million</td>
</tr>
<tr>
<td>Willful neglect and not corrected</td>
<td>$50,000 per violation, with an annual maximum of $1,000,000</td>
<td>$50,000 per violation, with an annual maximum of $1.5 million</td>
</tr>
</tbody>
</table>

### HIPAA ENFORCEMENT CRIMINAL

<table>
<thead>
<tr>
<th>Type of Violation</th>
<th>Criminal Penalty</th>
</tr>
</thead>
<tbody>
<tr>
<td>Covered entities and specified individuals who “knowingly” obtain or disclose PHI outside Privacy standards</td>
<td>A fine of up to $50,000; Imprisonment up to 1 year</td>
</tr>
<tr>
<td>Offenses committed under false pretenses</td>
<td>A fine of up to $100,000; Imprisonment up to 5 years</td>
</tr>
<tr>
<td>Offenses committed with the intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain or malicious harm</td>
<td>A fine of up to $250,000; Imprisonment up to 10 years</td>
</tr>
</tbody>
</table>
Establish an environment that emphasizes rock-solid compliance administration

Establish a strong Privacy/Security infrastructure
- Written Documentation
- Training/Communication
- Auditing
- Reporting
- Timely Corrective Action
- Embed Privacy/Security into Human Resource administration
MECHANICS OF HIPAA COMPLIANCE

- Establish Privacy/Security Official roles
- Establish a Compliance Committee
- Corporate Compliance policies and procedures:
  - Delineate the roles of Compliance Officials and Committee
  - Incorporate State Privacy regulations
  - Define organization’s expectations re: employee, volunteer, board and subcontractors’ conduct re Privacy standards
  - Clearly outline sanctions, enforcement standards, reporting breaches, anonymous reporting, corrective actions, audit/monitoring standards, training, communication standards, etc.

Sharon’s Quick & Dirty HIPAA Privacy & Security Checklist

<table>
<thead>
<tr>
<th>Y/N</th>
<th>Question</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Does your organization ensure that its risk management program restricts the impermissible use and disclosure of PHI?</td>
</tr>
<tr>
<td></td>
<td>Has your organization developed, documented, and implemented policies and procedures for assessing and managing risk for all forms of PHI?</td>
</tr>
<tr>
<td></td>
<td>Does your organization have policies and procedures that authorize members of your workforce to have access to PHI and describe the types of access that are permitted?</td>
</tr>
<tr>
<td></td>
<td>When a workforce member’s employment is terminated and/or a relationship with a business associate is terminated?</td>
</tr>
<tr>
<td></td>
<td>Does your organization have policies and procedures for contingency plans to provide access to PHI to continue operations after a natural or human-made disaster?</td>
</tr>
<tr>
<td></td>
<td>Does your organization have an emergency mode operations plan to ensure the continuation of critical business processes that must occur to protect the availability and security of PHI immediately after a crisis situation?</td>
</tr>
<tr>
<td></td>
<td>Does your organization have senior-level personnel responsible to develop and implement privacy/security policies and procedures? Do these staff have responsibility to decide who can access PHI (and under what conditions) and to create PHI access rules that others can follow?</td>
</tr>
<tr>
<td></td>
<td>Does your organization have a training program that requires that each board member/staff/volunteer (including temporary/contingent staff) with access to PHI is trained on privacy/security measures to reduce the risk of improper access, uses, and disclosures?</td>
</tr>
<tr>
<td></td>
<td>Does your organization keep records that detail when board/member/staff/volunteers satisfy fully completed periodic training?</td>
</tr>
<tr>
<td></td>
<td>Does your organization maintain a list of all of its subcontracted network, identifying which have access to your organization’s facilities, information systems and PHI?</td>
</tr>
<tr>
<td></td>
<td>Do you execute a BAA (or similar document) with your subcontracted networks that use/disclose PHI to transact business on your behalf requiring them to follow Privacy/Security regulations? How do you verify compliance?</td>
</tr>
<tr>
<td></td>
<td>Do your subcontracted network Agreements include provisions for immediate reporting of privacy/security breaches to your organization?</td>
</tr>
<tr>
<td></td>
<td>Does your organization have policies and procedures that describe how to position workstations to limit the ability of unauthorized individuals to view PHI?</td>
</tr>
<tr>
<td></td>
<td>Does your organization maintain a record of use/locations of hardware and media and the staff responsible for the use and security of the devices or media containing PHI use offsite?</td>
</tr>
</tbody>
</table>
BIBLIOGRAPHY

- Health IT  www.healthit.gov
- Public Law 104-191, HIPAA, Title II Administrative Simplification
- Public Law 111-5, American Recovery and Reinvestment Act, 2009
- HIPAA Violations information from Wikipedia

THANK YOU!

Sharon R. Williams  
CEO  
Williams Jaxon Consulting, LLC  
sharonr.williams@comcast.net  
313-516-3326
QUESTIONS & ANSWERS:
PLEASE SUBMIT USING THE "QUESTIONS" BOX

Aging and Disability Business Institute