JEFFERSON COUNTY COMMISSION HIPAA TRAINING

Employee Benefits & Executive Compensation Practice Group
Maynard Cooper & Gale PC
1901 6th Avenue North
Regions Harbert Plaza
Birmingham, Alabama 35203
(205) 254-1000

September, 2013

MAYNARD COOPER & GALE PC
ATTORNEYS AT LAW

© Maynard, Cooper & Gale, P.C. 2013

HIPAA Privacy Rules

- Health information held by an employer in its role as an employer is not protected
- Health information held by a plan sponsor must be handled confidentially and never used to make employment decisions
- Plan sponsors must act reasonably and within the scope of HIPAA when handling PHI

© Maynard, Cooper & Gale, P.C. 2013

MAYNARD COOPER & GALE PC
ATTORNEYS AT LAW

Why Must You Comply?

- Civil Penalties*
  - $100-$50,000 if the Covered Entity did not know, and by exercising diligence would not have known, of the violation
  - $1,000-$50,000 if the violation was due to reasonable cause and not willful neglect
  - $10,000-$50,000 if the violation was due to willful neglect, but was corrected
  - Minimum of $50,000 if the violation was due to willful neglect and was not corrected
  - Maximum of $1.5 million for all violations of an identical requirement or prohibition during a calendar year

*Applies to both Covered Entities and Business Associates

© Maynard, Cooper & Gale, P.C. 2013

MAYNARD COOPER & GALE PC
ATTORNEYS AT LAW

Why Must You Comply?

- Criminal Penalties*
  - Knowing and willful violations: maximum $50,000 fine and/or 1 year imprisonment
  - Violation committed under false pretenses: maximum $100,000 fine and/or 5 years imprisonment
  - Violation with intent to sell, transfer or use for commercial advantage, personal gain or malicious harm: maximum $250,000 fine and/or 10 years imprisonment

* Applies to both Covered Entities and Business Associates

© Maynard, Cooper & Gale, P.C. 2013

Why Must You Comply?

- State Attorney General may bring civil actions on behalf of state residents with penalties of up to $100/violation, with a cap of $25,000 for identical violations in the calendar year
- Violations may trigger private right of action under ERISA
- Promotes good employee relations

© Maynard, Cooper & Gale, P.C. 2013

To Whom Does HIPAA Apply?

Covered Entities

- Health Plans
  - Includes most employee welfare benefit plans that provide health care
  - Excludes self-administered plans with fewer than 50 participants
  - Excludes plans offering only certain types of coverage in which health care is provided as only a secondary or incidental benefit
- Health Care Clearinghouses
  - Entities that process information between standard and non-standard formats
- Health Care Providers
  - If they transmit health information electronically in connection with certain HIPAA transactions
- Business Associates

© Maynard, Cooper & Gale, P.C. 2013

What Are HIPAA's Privacy Standards Intended to Do?

- Control uses and disclosures of PHI by Covered Entities
- Establish basic rights for individuals
- Require Covered Entities to implement administrative policies, procedures and processes
- Preempt less stringent state law
- Restrict disclosures of PHI to, and uses and disclosures of PHI by, plan sponsors
- Reduce burdens on fully-insured group health plans which receive only limited PHI

© Maynard, Cooper & Gale, P.C. 2013

MAYNARD COOPER & GALE PC ATTORNEYS AT LAW

Terms to Understand:

- Use and Disclosure
- Individual
- Protected Health Information or PHI

© Maynard, Cooper & Gale, P.C. 2013

MAYNARD COOPER & GALE PC ATTORNEYS AT LAW

"Use" and "Disclosure"

- Use: Sharing, employment, application, utilization or analysis within a Covered Entity
- Disclosure: Release, transfer, provision of access to, or divulging in any other manner of information outside the Covered Entity

© Maynard, Cooper & Gale, P.C. 2013

MAYNARD COOPER & GALE PC ATTORNEYS AT LAW

"Individual"

- Generally, the person who is the subject of PHI
- Special rules for:
  - Deceased individuals
  - Personal representatives of adults or emancipated minors
  - Unemancipated minors
  - Abuse, neglect and endangerment situations

© Maynard, Cooper & Gale, P.C. 2013

MAYNARD COOPER & GALE PC ATTORNEYS AT LAW

"Protected Health Information"

- Protected health information ("PHI") means *individually identifiable health information* that is transmitted or maintained in any form
- Individually Identifiable Health Information ("IIHI") means information that:
  - Is created or received by a health care provider, health plan, employer or health care clearinghouse;
  - Relates to the physical or mental health or condition of an individual; the provision of health care to an individual; or the payment for the provision of health care to an individual; and
  - Either identifies the individual or there is a reasonable basis to believe that it could be used to identify the individual.
- IIHI in the employment records of an employer in its role as an employer is <u>not</u> PHI

© Maynard, Cooper & Gale, P.C. 2013

MAYNARD COOPER & GALE PC ATTORNEYS AT LAW

What Are Business Associates?

- Performs, on Covered Entity's behalf, an activity involving the use or disclosure of PHI
- Provides, to a Covered Entity, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation or financial services involving the disclosure of PHI
- Does not include members of a Covered Entity's workforce or certain financial institutions
- Entities that transmit PHI for Covered Entities and require routine access to PHI (e.g., Health Information Exchange Organization)
- Vendor that contracts with a Covered Entity to provide a personal health record to patients as part of the entity's electronic health record

© Maynard, Cooper & Gale, P.C. 2013

MAYNARD COOPER & GALE PC ATTORNEYS AT LAW

How Do Covered Entities Relate to Business Associates?

- Covered Entity may disclose PHI to a Business Associate if the Covered Entity has satisfactory assurances from the Business Associate that it will safeguard the information
- Covered Entities are required to enter into contracts with Business Associates to ensure that Business Associates comply with HIPAA rules
- Business Associates are now directly liable for compliance with HIPAA privacy and security rules

© Maynard, Cooper & Gale, P.C. 2013

How Does HIPAA Regulate the Use and Disclosure of PHI?

- General Rule: No use or disclosure of PHI unless permitted or required by the Privacy Rules or the rules concerning compliance and enforcement
  - Mandatory Disclosures
    - To the individual for access and accounting
    - To the Department of Health & Human Services ("DHHS") for compliance and enforcement
  - Permitted Uses and Disclosures

© Maynard, Cooper & Gale, P.C. 2013

Permitted Uses and Disclosures:

- Without permission to the individual
- Without permission for treatment, payment or health care operations
- Without permission if the individual has an opportunity to agree or object
- Without permission for national priority purposes
- With permission in the form of an authorization

© Maynard, Cooper & Gale, P.C. 2013

Special Rules Governing Uses and Disclosures

- Minimum necessary standard
- De-identification of PHI and limited data sets
- Psychotherapy notes

© Maynard, Cooper & Gale, P.C. 2013

MAYNARD COOPER & GALE PC
ATTORNEYS AT LAW

Disclosure of PHI by Group Health Plan to Plan Sponsor

Requires Amendments to Plan Documents

- Establish plan sponsor's permitted and required uses and disclosures
- Prohibit disclosures to plan sponsor absent certification from plan sponsor
  - Plan sponsor will not use or disclose PHI other than as permitted or required by plan documents or law
  - Plan sponsor will pass on restrictions to its agents and subcontractors
  - Plan sponsor will not use or disclose PHI for employment-related actions or in connection with other benefits
- Require adequate separation between plan and plan sponsor

© Maynard, Cooper & Gale, P.C. 2013

MAYNARD COOPER & GALE PC
ATTORNEYS AT LAW

Disclosures of PHI by Group Health Plan to Plan Sponsor Are Permitted if:

- Disclosures of Summary Health Information for purpose of obtaining premium bids or modifying or terminating the plan
- Disclosures of enrollment and disenrollment information

© Maynard, Cooper & Gale, P.C. 2013

MAYNARD COOPER & GALE PC
ATTORNEYS AT LAW

For What Purposes May a Plan Use and Disclose PHI to Plan Sponsor?

- For plan sponsor's proper administrative functions
- Notice of Privacy Practices must alert individuals if PHI is to be disclosed to the plan sponsor
- May not disclose PHI to the plan sponsor for employment-related decisions or in connection with other benefits

© Maynard, Cooper & Gale, P.C. 2013

MAYNARD COOPER & GALE PC
ATTORNEYS AT LAW

Individuals' Rights

- Notice of Privacy Practices
- Inspection and copying of PHI
  - Covered Entities now have 30 days to respond (prior rule was 60-90 days)
  - Covered Entities may request a one-time extension of up to 30 additional days upon provision of written notice to the individual, including the reason for the delay and the expected date of completion

© Maynard, Cooper & Gale, P.C. 2013

MAYNARD COOPER & GALE PC
ATTORNEYS AT LAW

Individuals' Rights

- Accounting of disclosures of PHI
- Amendment and correction of PHI
- Right to request additional privacy protections restricting PHI disclosures

© Maynard, Cooper & Gale, P.C. 2013

MAYNARD COOPER & GALE PC
ATTORNEYS AT LAW

Information Safeguards

- Administrative procedures
- Personnel designations
- Training
- Complaints process
- Sanctions
- Mitigation of harm

© Maynard, Cooper & Gale, P.C. 2013

Information Safeguards

- Refraining from intimidating or retaliatory acts
- No waiver of rights
- Policies and procedures
- Administrative, technical and physical safeguards
- Oral communications
- Documenting compliance

© Maynard, Cooper & Gale, P.C. 2013

What Happens When Something Goes Wrong?

- The Health Information Technology for Economic and Clinical Health Act ("HITECH Act") introduced detailed breach notification requirements triggered by a breach of "unsecured PHI"
- Notice to affected individuals and to the DHHS
- Large breaches (500+ persons) require notice to the media

© Maynard, Cooper & Gale, P.C. 2013

What Constitutes a Breach?

- An impermissible use or disclosure of PHI is presumed to be a breach unless the Covered Entity or Business Associate demonstrates that there is a low probability that the PHI has been compromised

© Maynard, Cooper & Gale, P.C. 2013

MAYNARD COOPER & GALE PC
ATTORNEYS AT LAW

What Constitutes a Breach?

- Probability of harm must be assessed by considering at least:
  - The nature and extent of PHI involved
  - The unauthorized person who used the PHI or to whom the disclosure was made
  - Whether PHI was actually acquired or viewed
  - The extent to which the risk to PHI has been mitigated

© Maynard, Cooper & Gale, P.C. 2013

MAYNARD COOPER & GALE PC
ATTORNEYS AT LAW

Risk Assessment Factors to Consider

- 1. The Nature and Extent of the PHI involved, including the types of identifiers and likelihood of re-identification.
  - What type of PHI was involved?
  - Was it sensitive in nature?
  - Could the PHI be used by an unauthorized user in a manner adverse to the individual?
  - What is the likelihood that the PHI released could be re-identified based on the context and the ability to link the information with other available information?

© Maynard, Cooper & Gale, P.C. 2013

MAYNARD COOPER & GALE PC
ATTORNEYS AT LAW

Risk Assessment Factors to Consider

- 2. The unauthorized person who used the PHI or to whom the disclosure of PHI was made.
  - Does the unauthorized person who received the information have obligations to protect the privacy and security of the information?
  - Could the unauthorized person who received the PHI re-identify the information?

© Maynard, Cooper & Gale, P.C. 2013

MAYNARD COOPER & GALE PC ATTORNEYS AT LAW

Risk Assessment Factors to Consider

- 3. Whether the PHI was actually viewed or acquired or, alternatively, if only the opportunity existed for the information to be viewed or acquired.
  - If PHI was never accessed, viewed, acquired, transferred or otherwise compromised, the covered entity could determine that the information was not actually acquired by an unauthorized individual even though the opportunity existed.

© Maynard, Cooper & Gale, P.C. 2013

MAYNARD COOPER & GALE PC ATTORNEYS AT LAW

Risk Assessment Factors to Consider

- 4. The extent to which the risk has been mitigated.
  - Covered entities should attempt to mitigate the risks following any impermissible use or disclosure, such as by obtaining the recipient's satisfactory assurances that the information will not be further used or disclosed (through a written confidentiality agreement or similar means) or will be destroyed.

© Maynard, Cooper & Gale, P.C. 2013

MAYNARD COOPER & GALE PC ATTORNEYS AT LAW

HIPAA Security Rules

"Electronic Protected Health Information" is PHI that is transmitted or stored in Electronic Media ("EPHI")

- Electronic Media:
  - Electronic storage media
  - Electronic transmission
  - Certain transmissions of paper and voice are not EPHI
- EPHI is limited to such information that is created, received maintained, or transmitted by or on behalf of the Covered Entity

© Maynard, Cooper & Gale, P.C. 2013

MAYNARD COOPER & GALE PC ATTORNEYS AT LAW

HIPAA Security Rules

- Required documents
  - Risk analysis
  - Policies and procedures
  - Plan amendment
  - Business associate agreements
  - Security official designation
  - Addressable implementation specification analysis
  - Security incident tracking

© Maynard, Cooper & Gale, P.C. 2013

MAYNARD COOPER & GALE PC ATTORNEYS AT LAW

HIPAA Generally Requires That the Covered Entity:

- Authorize and supervise EPHI access of employees responsible for the administration of the Covered Entity
  - Workforce clearance procedure
  - Termination procedures:
    - Employees who are terminated or whose EPHI access is terminated must return all access devices and data that is solely under the employee's control
    - Such employee's user ID and password must be disabled

© Maynard, Cooper & Gale, P.C. 2013

MAYNARD COOPER & GALE PC ATTORNEYS AT LAW

HIPAA Generally Requires That the Covered Entity:

- Ensure the confidentiality, integrity, and availability of all EPHI
- Protect against any reasonably anticipated threats or hazards to the security or integrity of such EPHI
- Protect against any reasonably anticipated uses or disclosures of such EPHI that are not permitted or required by the Privacy Rule
- Ensure compliance with the HIPAA Security Rule by employees responsible for administration of the Covered Entity

© Maynard, Cooper & Gale, P.C. 2013

MAYNARD COOPER & GALE PC ATTORNEYS AT LAW

HIPAA Generally Requires That the Covered Entity:

- Document actions, activities, or assessments required under the Security Standards
  - Must be in written (which may be electronic) form
  - Must be retained for 6 years after the later of the date it was created or the date it was last in effect
  - Must be available to employees responsible for plan administration
  - Must be reviewed periodically and updated as needed

© Maynard, Cooper & Gale, P.C. 2013

MAYNARD COOPER & GALE PC ATTORNEYS AT LAW

HIPAA Generally Requires that the Covered Entity:

- Distribute periodic security updates and reminders
- Maintain employee education programs with respect to:
  - Guarding against, detecting and reporting malicious software
  - Monitoring log-in attempts and reporting discrepancies
  - Creating, changing, and safeguarding passwords
- Periodically review employees' EPHI access rights and modify as necessary to limit access to the minimum necessary

© Maynard, Cooper & Gale, P.C. 2013

MAYNARD COOPER & GALE PC ATTORNEYS AT LAW

Physical Safeguards Must Be Implemented

- Limit physical access to all workstations with EPHI access and other EPHI systems to restrict access to authorized employees
- Implement procedures for the receipt and removal of hardware and electronic media containing EPHI
- Address re-use and final disposition of electronic media containing EPHI

© Maynard, Cooper & Gale, P.C. 2013

MAYNARD COOPER & GALE PC
ATTORNEYS AT LAW

Technical Safeguards Must Be Implemented

- Prevent unauthorized access to EPHI on electronic network
- Develop technical policies and procedures:
  - Protect EPHI from alteration or destruction
  - Verify identity of person or entity seeking access to EPHI
  - Control EPHI access with unique user identification, emergency access procedure, automatic logoff and encryption

© Maynard, Cooper & Gale, P.C. 2013

MAYNARD COOPER & GALE PC
ATTORNEYS AT LAW

Employer/Plan Sponsor Issues

- Claims advocacy on behalf of employees
- Enrollment information
- Medical information and employment records
- Accounting of disclosures
- Disclosures of an individual's PHI to persons other than the individual
- Workforce training

© Maynard, Cooper & Gale, P.C. 2013

MAYNARD COOPER & GALE PC
ATTORNEYS AT LAW

Assisting Employees with Benefits Questions

- No disclosure to the employer of an individual's PHI without the individual's authorization
- Except for disclosures relating to plan administration
  - Treatment
  - Payment
  - Health care operations

© Maynard, Cooper & Gale, P.C. 2013

MAYNARD COOPER & GALE PC ATTORNEYS AT LAW

Assisting Employees with Benefits Questions

- Any member of the employer's workforce may discuss an employee's claim for benefits with the employee without an authorization
- No disclosure of an employee's PHI **from the health plan** without an authorization
- No disclosure of an employee's PHI **from a third-party administrator** without an authorization

© Maynard, Cooper & Gale, P.C. 2013

MAYNARD COOPER & GALE PC ATTORNEYS AT LAW

Enrollment Information

- The health plan may disclose enrollment information to the employer without an authorization

© Maynard, Cooper & Gale, P.C. 2013

MAYNARD COOPER & GALE PC ATTORNEYS AT LAW

Medical Information May Not Be PHI

- Medical information held by the employer in its role as an employer is not PHI
- Examples:
  - Records relating to
    - Occupational injury
    - Disability insurance eligibility
    - Sick leave requests and justifications
    - Drug screening test results
    - Workplace medical surveillance
    - Fitness for duty tests

© Maynard, Cooper & Gale, P.C. 2013

Accounting of Disclosures

- General rule
  - Track disclosures of an individual's PHI
  - Maintain record of a disclosure for 6 years after the date of disclosure (3 years for an electronic health record)
  - Provide record of disclosures to an individual upon the individual's request
  - If you maintain records in electronic form, you must provide access in the electronic form upon the individual's request

© Maynard, Cooper & Gale, P.C. 2013

Accounting of Disclosures

- Required content of an accounting of disclosures
  - Date of the disclosure
  - The name and address (if known) of the entity or person who received PHI
  - A brief description of the disclosed PHI
  - A brief statement of the purpose of the disclosure
- Special rule for multiple disclosures
  - Frequency or number of disclosures made during the accounting period
  - Date of the last disclosure during the accounting period

© Maynard, Cooper & Gale, P.C. 2013

Accounting of Disclosures

- Exceptions to the accounting requirements
  - Disclosures for plan administration
  - Disclosures made to an individual
  - Disclosures that are authorized
  - Disclosures for national security or intelligence purposes
  - Disclosures to correctional institutions or law enforcement officials
  - Disclosures as part of a limited data set
  - Disclosures that are incidental to a permissible use or disclosure
  - Disclosures to persons involved in the individual's care or payment for care

© Maynard, Cooper & Gale, P.C. 2013

Restrictions on Marketing Communications

- In general, **authorization** is required for plan to send **communication that encourages individual to purchase or use a product or service**
- If the communication is for treatment or health care operations, authorization is required if the plan or a business associate **receives financial remuneration for making the communication**
- Types of affected communications:
  - Information about provider or the plan network
  - Discounts or coupons for health products or services
  - New or improved plan benefits

© Maynard, Cooper & Gale, P.C. 2013

Restrictions on Marketing Communications

- Exceptions to authorization requirement, even if financial remuneration is paid
  - **Face-to-face communications**
  - Promotional gift of **nominal value**
  - **Promoting good health in general**
  - Information about **government programs** such as Medicare and Medicaid
- Exceptions to authorization requirement where financial remuneration is limited to **reasonable cost of making the communication (no profit)**
  - Information about generic drugs
  - Refill reminders
  - Reminders to take medicine
  - For self-administered or biologic drugs, information about the drug delivery system (e.g., insulin)

© Maynard, Cooper & Gale, P.C. 2013

Restrictions on the Sale of PHI

- **General prohibition on sale of PHI without authorization**
- The authorization must acknowledge that the **plan or business associate will receive payment (remuneration) for disclosing PHI**
- Payment can be **direct or indirect**, and includes non-financial (in-kind) remuneration
- There are exceptions, including for treatment and payment purposes, reasonable cost of providing permitted disclosures, and cost of providing access to PHI or an accounting of disclosures

© Maynard, Cooper & Gale, P.C. 2013

MAYNARD COOPER & GALE PC ATTORNEYS AT LAW

When Is it Permissible to Disclose an Individual's PHI to Others?

- Spouses and other family members
  - Involved in the individual's care or payment for care
  - Opportunity to agree or object to disclosure
  - Special case: restrictions on disclosures

© Maynard, Cooper & Gale, P.C. 2013

MAYNARD COOPER & GALE PC ATTORNEYS AT LAW

When Is it Permissible to Disclose an Individual's PHI to Others?

- Parents of minor children
  - Same rights as a child
  - Personal representatives and court-appointed guardians
  - Special case: non-custodial parents
- Verification
  - Identity
  - Authority

© Maynard, Cooper & Gale, P.C. 2013

MAYNARD COOPER & GALE PC ATTORNEYS AT LAW

HIPAA Requires This Training!

- Amount of training
- Ongoing training
  - New employees
  - Changes in the law
- Certifications of training should be obtained

© Maynard, Cooper & Gale, P.C. 2013

Glossary

- DHHS: Department of Health & Human Services
- EPHI: Electronic Protected Health Information
- ERISA: Employee Retirement Income Security Act of 1974
- HIPAA: Health Insurance Portability & Accountability Act of 1996
- IIHI: Individually Identifiable Health Information
- PHI: Protected Health Information

© Maynard, Cooper & Gale, P.C. 2013

MAYNARD COOPER & GALE PC
ATTORNEYS AT LAW

1901 Sixth Avenue North 2400 Regions Harbert Plaza Birmingham, Alabama 35203-2618 205.254.1000 Fax 205.254.1999
www.maynardcooper.com
© Maynard, Cooper & Gale, P.C. 2013