

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

2

Maynard Cooper & Gale pc

Why Must You Comply?

Civil Penalties*

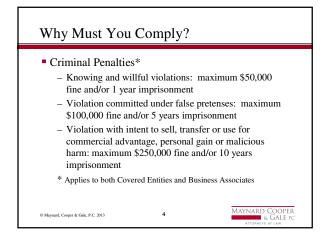
© Maynard, Cooper & Gale, P.C. 2013

© Maynard, Cooper & Gale, P.C. 2013

- \$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

3

MAYNARD COOPER & GALE PC



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 calend gear
- Violations may trigger private right of action under ERISA

5

Promotes good employee relations

To Whom Does HIPAA Apply?

Covered Entities

© Maynard, Cooper & Gale, P.C. 2013

- 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

6

MAYNARD D COOPER & GALE pc

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

© Maynard, Cooper & Gale, P.C. 2013

 Restrict disclosures of PHI to, and uses and disclosures of PHI by, plan sponsors

>) COOPER & GALE pc

D COOPER & GALE po

 Reduce burdens on fully-insured group health plans which receive only limited PHI

7

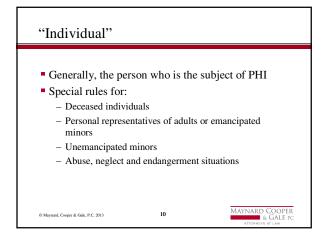
Terms to Understand:
Use and Disclosure
Individual
Protected Health Information or PHI

"Use" and "Disclosure"

© Maynard, Cooper & Gale, P.C. 2013

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

9



"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; or the Either identifies the individual extension to be a seen to be 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 not PHI

11

© Maynard, Cooper & Gale, P.C. 2013

© Maynard, Cooper & Gale, P.C. 2013

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

12

Maynard Cooper & Gale pc

© COOPER & GALE pc

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 <u>directly liable</u> for compliance with HIPAA privacy and security rules

13

© Maynard, Cooper & Gale, P.C. 2013

Maynard Cooper & Gale pc

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

Permitted Uses and Disclosures:

Without permission to the individual

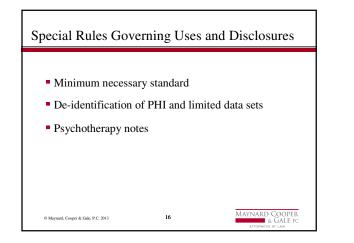
© Maynard, Cooper & Gale, P.C. 2013

- <u>Without</u> permission for treatment, payment or health care operations
- <u>Without</u> permission if the individual has an opportunity to agree or object
- Without permission for national priority purposes

15

• With permission in the form of an authorization

Maynard Cooper & Gale pc





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

18

© Maynard, Cooper & Gale, P.C. 2013

MAYNARI

D COOPER & GALE pc

• Disclosures of enrollment and disenrollment information

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

19

 May not disclose PHI to the plan sponsor for employment-related decisions or in connection with other benefits

© Maynard, Cooper & Gale, P.C. 2013

NARD COOPER & GALE pc

& GALE PC

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

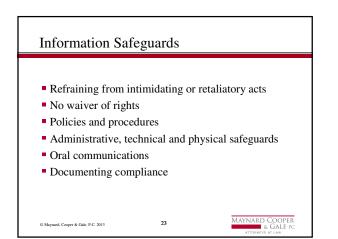
Individuals' Rights

© Maynard, Cooper & Gale, P.C. 2013

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

21





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

24

© Maynard, Cooper & Gale, P.C. 2013

MAYNARE

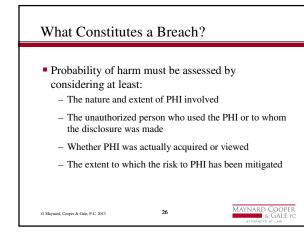
What Constitutes a Breach?

 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 <u>low probability</u> that the PHI has been compromised

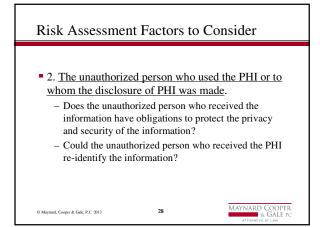
25

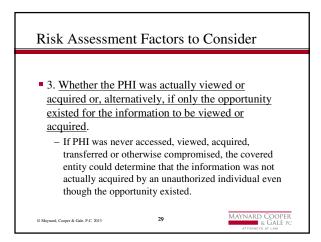
© Maynard, Cooper & Gale, P.C. 2013

NARD COOPER & GALE pc



<section-header><list-item><list-item><list-item><list-item><list-item><list-item><list-item></table-row></table-row></table-row></table-row></table-row></table-row></table-row></table-row></table-row></table-row></table-row></table-row></table-row></table-row></table-row></table-row></table-row>





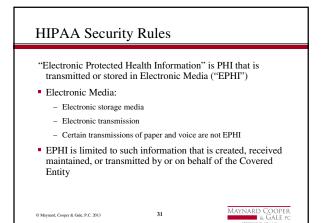
Risk Assessment Factors to Consider

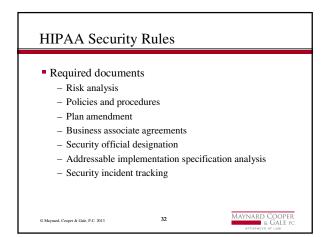
• 4. The extent to which the risk has been mitigated.

 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.

30

© Maynard, Cooper & Gale, P.C. 2013





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

Maynard Cooper & Gale pc

· Such employee's user ID and password must be disabled



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

34

© Maynard, Cooper & Gale, P.C. 2013

Maynard Cooper & Gale pc

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 35

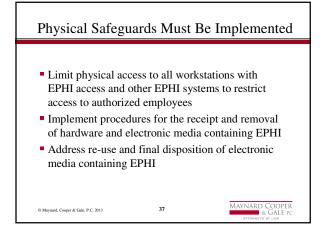
HIPAA Generally Requires that the Covered Entity:

- 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

36

© Maynard, Cooper & Gale, P.C. 2013

MAYNARD COOPEF & GALE po



Employer/Plan Sponsor Issues

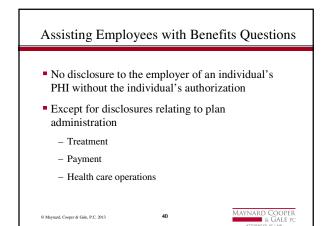
- Claims advocacy on behalf of employees
- Enrollment information
- Medical information and employment records
- Accounting of disclosures
- Disclosures of an individual's PHI to persons other than the individual

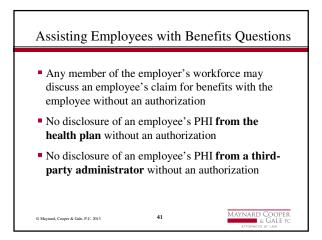
39

Workforce training

© Maynard, Cooper & Gale, P.C. 2013

Maynard Cooper & Gale pc





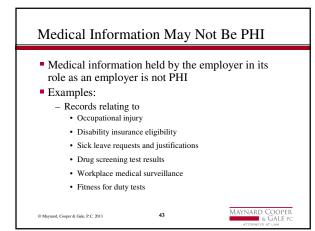
Enrollment Information

© Maynard, Cooper & Gale, P.C. 2013

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

42

Maynard Co & Ga



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

44

© 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

© Maynard, Cooper & Gale, P.C. 2013

- Frequency or number of disclosures made during the accounting period
- Date of the last disclosure during the accounting period

45 MAYNARD COOPER & GALE PC

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 COOPER & GALE PC

46

© Maynard, Cooper & Gale, P.C. 2013



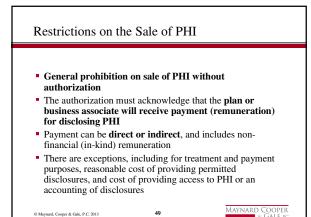
Restrictions on Marketing Communications

· Exceptions to authorization requirement, even if financial remuneration is paid

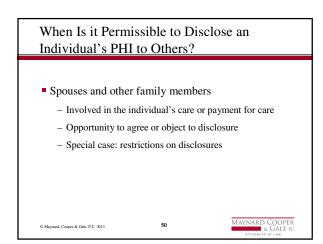
- Face-to-face communications
- Promotional gift of nominal value
- Promoting good health in general
- Information about government programs such as Medicare and Medicaid Exceptions to authorization requirement where financial remuneration is
- limited to reasonable cost of making the communication (no 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) 48

© Maynard, Cooper & Gale, P.C. 2013

MAYNARD D COOPER & GALE pc



) COOPER & GALE pc



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

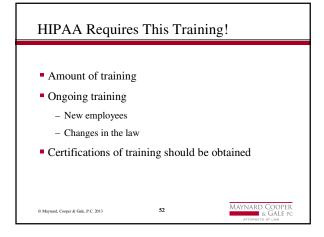
- Parents of minor children
 - Same rights as a child
 - Personal representatives and court-appointed guardians

51

- Special case: non-custodial parents
- Verification
- Identity
- Authority

© Maynard, Cooper & Gale, P.C. 2013

d Cooper & Gale pc



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

53

PHI: Protected Health Information

© Maynard, Cooper & Gale, P.C. 2013

MAYNARD COOPER & GALE PC

MAYNARD COOPER & GALE PC ATTORNEYS AT LAW 1015104 Avenue No. 2007 Represe Hener Plan Resemption. Addam 2003-2013 2013-20100 Fer 20131-109