OBER | KALER

HEALTH CARE | GENERAL COUNSEL INSTITUTE

# Foundations in HIPAA

*Building Blocks of Health Law*

**January 22, 2014**

OBER | KALER

HEALTH CARE | GENERAL COUNSEL INSTITUTE

www.healthcaregcinstitute.com

# Welcome

- Housekeeping
- Today's speakers
- Overview of the topic
- Discussion
- Questions

# Welcome

- Download the slides for today's program by clicking the PDF link in the upper left corner of your screen.

- Also on the left is a Q&A box where you may type your questions. We'll look at those questions at the end of the program and answer as many as we can.

- At the end of the program, you'll receive an email with a link to a survey. Please take a moment to fill that out and give us your feedback.

# Meet Today's Speakers

Sarah E. Swank
Principal, Ober|Kaler
seswank@ober.com
202.326.5003

Emily H. Wein
Principal, Ober|Kaler
ehwein@ober.com
410.347.7360

James B. Wieland
Principal, Ober|Kaler
jbwieland@ober.com
410.347.7397

**Join us on LinkedIn:**
**Ober|Kaler Health Care General Counsel Institute Group**

# Foundations

- The Ober|Kaler Health Care General Counsel Institute is pleased to introduce its *Foundations* series, a collection of programs designed to equip in house counsel with a solid foundation in the cornerstones of health law. The series is for in house counsel who are:
  - beginning their careers
  - experienced counsel working outside of health law
  - experienced in health law and want to get up to speed in areas outside of their niches
  - experienced health law counsel who would like refreshers on current law and developing trends

# HIPAA Overview: "Administrative Simplification"

- The Health Insurance Portability and Accountability Act of 1996 (HIPAA).
- Standardization across payers of 9 basic transactions including claims, electronic remittance advice, eligibility, authorization, pharmacy, enrollment, coordination of benefits, attachments and first notice of claim.

# HIPAA Overview

- Security of electronic health information and electronic signatures.
- Privacy of individually identifiable patient information.

# Reasons to Comply

WHY?

- Moral imperative: Protecting patient records is the right thing to do and is a major concern of patients.
- Business imperative: Protecting patient information is the right thing to do; it will be become a competitive advantage.
- Legal imperative: Protecting the radiology practice from litigation is the right thing to do. (Significant penalties imprisonment of 1-5 years and fines of $50,000 – 250,000).

# Enforcement Provisions

- HHS Office of Civil Rights will handle all HIPAA compliance issues, including:
  - Imposing civil penalties and making referrals for criminal prosecution,
  - Making exception determinations,
  - Responding to questions regarding the rules and providing interpretation and guidance,
  - Overseeing voluntary compliance through technical assistance and other means, and
  - Responding to state requests for exception determinations.

# HIPAA from 40,000 feet

- A new way of relating to the practice's patients, centered around new patient rights
- Impact on **internal *uses*** and ***disclosures***, not just external disclosures
- The "Business Associate" concept
- New infrastructure requirements
- A new internal culture of privacy

# PART I: HIPAA Privacy Standards

- Final : Compliance Required April 2003
- Does not preempt state law or other federal law; establishes a statutory “floor” for privacy.
- Any State law or regulation that is contrary and more “stringent” is not preempted (e.g., mental health, AIDS/HIV, substance abuse).

# Scope – What are the Limits of Coverage?

- What's Covered? – Protected Health Information (PHI)
  - Individually identifiable health information that is transmitted or maintained in any form or medium.
- De-identified Information is not covered
- Two methods:
  - Generally accepted statistical and scientific methods.
  - Remove the identifiers of the individual, relatives, employers and household members.

# Scope - Who is Covered: Covered Entities

- Health Care Providers who transmit any health information in electronic form in connection with a covered transaction.
- Health Plans
  - Group health plan qualifying under ERISA, that have fifty or more participants.
  - Health insurance issuer.
  - Health maintenance organization.
  - Medicare Part A and B, Medicaid title 19.
- Clearinghouses
  - Any entity, including billing services, repricing companies, community health management information systems and value added networks.

# Scope - Business Associates and Business Associate Contracts

- "Covered Entities" are limited to provider organization that transmits any of the nine-named transactions, payers and clearinghouses.
- A "Business Associate" is any entity that performs services to or on behalf of a covered entity and that uses or discloses protected health information that belongs to the covered entity

# Business Associate Contracts

- Covered entities must have a Business Associate Contract with their business associates that binds the Business Associate to:
  - Comply with the covered entities' privacy practices.
  - Provide protections for any PHI that it receives from the Covered Entity.

# Business Associate Contracts

- Exceptions:
  - Disclosure of PHI to a health care provider for the purpose of treatment.
  - A conduit is not a business associate.
  - Participating in joint activities does not mean that one party is performing services to or on the behalf of another entity
  - Hospitals and their Medical Staffs are not “Business Associates” – they are in an “Organized Health Care Arrangement”.

# Business Associate Contract Required Terms

- Obligate the Business Associate:
  - not to use or disclose the PHI other than as permitted in the contract
  - to use appropriate safeguards to prevent use or disclosure of the information.
  - to report to the Covered Entity any use or disclosure of the information not provided for in the contract.
  - to ensure that any agents or subcontractors that the Business Associate provides PHI to agree to the same conditions and restrictions.
  - to make available PHI in accordance with the “access of individuals to PHI” provisions.

# Business Associate Contract Required Terms

  - to make the PHI available in accordance with "right to amend PHI" provisions of the rule.
  - to make its internal practices, books, and records relating to the use and disclosure available to the Secretary.
- At termination of the contract, if feasible, to return or destroy all PHI received. If the return is not feasible, to extend the protections.
- Authorize termination of the contract by the covered entity in the event the covered entity determines that the business associate has violated a material term of the contract.

# Control of Disclosures and Right to Access

- Minimum Necessary Disclosure / Use Provision:
  - With the exception of uses and disclosures for the purpose of treatment, any patient information used / disclosed be limited to the minimum amount necessary to accomplish purpose of disclosure.
  - Provider is responsible for determining the minimum amount needed.

# Individual's Control of their PH

- Covered entities must provide a Notice of Privacy Practices.
- With some exceptions, Covered entities must seek permission from the individual to use or disclose their PHI.
- "Consent" addresses the use and disclosure of PHI for "treatment", "payment" and "health care operations".
- Certain uses and disclosures require only an opportunity for the individual to agree or object, e.g. to family involved in care.

# Individual Control of their PHI

- "Authorization" essentially addresses the use of PHI for all other purposes.
- Exceptions:
  - Disclosures required by law and for other public purposes require neither consent or authorization.
  - Right of the individual to access, copy and amend their medial record.

# Consent

- "Payment": Any activity that is undertaken by a health plan to obtain premiums or fulfill its responsibility for coverage or health care providers' activities undertaken to obtain or provide reimbursement for the provision of health care.
- "Treatment": The provision, coordination, or management of health care and related services by one or more health care providers.

# Consent

- Health Care Operations:
  - Quality assessment and improvement activities.
  - Reviewing the competence or qualifications of health care professionals.
  - Medical review, legal services, and auditing functions.
  - Business planning and development.
  - Business management and general administrative activities
  - Creating de-identified health information, fundraising for the benefit of the covered entity, and marketing for which an individual authorization is not required.

# No Consent Required in "Indirect Treatment Relationships"

- Provider delivers health care "based on the orders of another health care provider; and
- "Typically" reports the diagnosis or results directly to another health care provider who reports to the individual
- Radiology cited by HHS as the example

# Authorization

- Required for all use and disclosure not required by law, for the purpose of public safety or covered under consent or right of an individual to agree or object.
- Must contain a statement that treatment may not be conditioned on an authorization, except research related treatment.

# Authorization

- A description of each purpose for which the PHI will be used or disclosed.
- Statement that the individual may refuse.
- Individual may revoke an authorization in writing at any time.
- A covered entity must document and retain authorizations.

# Individual Right to Request Restrictions

- An individual has the right to request from any covered entity.
- The covered entity may refuse to agree to the restrictions.
  - Restrictions must be documented and any documentation regarding restrictions must be retained for six years.

# Confidential Communication Requirements

- An individual may request a Covered Entity to provide confidential communication of PHI from the covered entity to the individual:
  - At their place of employment.
  - By mail to designated address.
  - By phone to a designated number.
  - Mail be sent in a closed envelope and not by post card.

# Right of Access and Amendment of Records

- Access
  - If possible, the Covered Entity must provide the information in the format requested by the individual and the individual may choose whether to inspect, copy or inspect and copy the information.
  - May charge reasonable “cost based” fees.
  - Exceptions for
    - psychotherapy notes.
    - disclosure may harm the individual or others under specific circumstances.

# Amendment

- A covered entity may deny a request for amendment if:
  - Entity did not create the PHI or record;
  - If the PHI is not part of a “Designated Record Set”;
  - If the information is determined to be accurate and complete.

# Right to an Accounting of Disclosures

- Disclosures made for purposes other than treatment, payment and health care operations for up to six years prior to the request for an accounting.
- The accounting must contain:
  - Date of each disclosure.
  - Name and address of the person or organization receiving the PHI.
  - Brief Description of the information disclosed.
  - The purpose for the disclosure.

# Administrative Requirements

- Privacy Officer.
- Training of employees.
- Privacy Policy & Procedures.
- Internal Complaint Process.
- Sanctions.
- Mitigation of Violations
- No Waiver of Rights is valid.

# Privacy Standards Action Steps

- Identify the responsible party / “Privacy Officer”;
- Inventory Protected Health Information: location, access, use and disclosure;
- Identify all “Business Associates”;
- Start training practice personnel to “Think Privacy”
- Muster available resources;
- Develop a plan and a time line

# HIPAA Security Standards

- Not final – published in proposed form only
- Administrative Procedures
  - A security audit/assessment and risk analysis.
  - Requirements include:
    - audit trail policy
    - certification
    - change control process
    - contract approval to include chain of trust language in trading partner agreements,
    - human resources orientation and termination,
    - information access privileges,
    - workstation location,
    - password and authentication policies and security incident procedures.

# HIPAA Security Standards

  - Contingency planning/disaster recovery (must be tested),
  - a formal business process control,
  - formal record processing,
  - security configuration documentation and appointment of a security officer.
- Employee and vendor education and training of security policy.

# HIPAA Security Standards

- Physical Safeguards
  - The ability to protect the computers and the physical records.
  - Each physical safeguard must be documented.
- Technical Security Services
  - Support or enforce the administrative policy and procedures.
  - Ensure the authentication of the user and restrict the user to only the systems, applications and data for which the user is authorized.

# HIPAA Security Standards

- Technical Security Mechanisms
  - Protections of patient data from public networks.
  - Appropriate deployment of communications/network controls.
  - Internet use monitoring.
  - Encryption.
  - Digital Certificates.
  - Virtual Private Networks.
  - Firewalls and Virus Protection.
  - On-going threat, penetration and vulnerability audits.

# HIPAA Security Standards

- HCFA Internet Security Policy details the level of encryption required
  - Essentially requires 112-bit asymmetric minimum.
- Electronic Signatures
  - Electronic signatures are not required.
  - If an electronic signature is used, the electronic signature used must be a true digital signature (as opposed to a scanned signature).
  - With properties that ensure message integrity, non-repudiation, and user authentication.

# Security Standards Action Steps

- Assign Security Responsibilities
- Perform a risk assessment
- Inventory information systems
- Set policies on workstations, medical records, and other PHI
- Educate practice employees – begin a culture of security awareness

# HIPAA Transaction Standards

- Compliance required as of October 2002
- Electronic standard for transactions constituting most health care administrative functions
  - Health care claim or encounter
  - Claim payment and remittance advice
  - Health care claim status
  - Coordination of benefits
  - Eligibility for a health plan

# HIPAA Transaction Standards

- Referral certification and authorization
- Enrollment and disenrollment
- Premium payments
- Claims attachments (to come)
- First report of injury (to come)

# Designated Code Standard

- International Classification of Diseases, 9th Edition, Clinical Modification (ICD-9-CM)
- Current Procedural Terminology, 4th Edition (CPT-4)
- Health Care Financing Administration Common Procedure Coding System (CPT-4)
- Code on Rental Procedures and Nomenclature, 2nd Edition (CDT-2)
- National Drug Codes (NDC)

# Designated Transaction Standards

- American National Standards Institute
- Institute (ANSI) Accredited Standards Committee X12 (ASC12)
- National Counsel for Prescription Drug Programs (NC PDP)

# Example: Health Care Claim or Encounter

- X12-837-Health Care Claim
- Similar to UB-92 or HCFA-1500 (for non-dental claims)
- Data sets may be different
- Data definitions are the same

# Example:
# Claims Payment and Remittance Advice

- X12-835-Health Care Claim Payment/Advice
- Like X12-837, already used by Medicare and some other payers
- If Provider and payer agree, X12-535 can be terminated to provider via provider's bank
  - Remittance advice
  - Value (electronic funds transfer like a bank)
- X12-835 carries significantly more data than paper claims
- Compliance implications
- Better matching payment to patient/service non-contracted plans/providers

# Transaction Standards Action Plan

- Inventory current claims, pre-authorization,etc for compliance
- Seek information from payors, hospitals and others as to their “when and how” as to accepting HIPAA compliant transactions

# Questions?

Type your questions into
the Q&A box on the left.

We'll answer as many as we can.

# More questions?

Sarah E. Swank
Principal, Ober|Kaler
seswank@ober.com
202.326.5003

Emily H. Wein
Principal, Ober|Kaler
ehwein@ober.com
410.347.7360

James B. Wieland
Principal, Ober|Kaler
jbwieland@ober.com
410.347.7397

**Join us on LinkedIn:**

**Ober|Kaler Health Care General Counsel Institute Group**