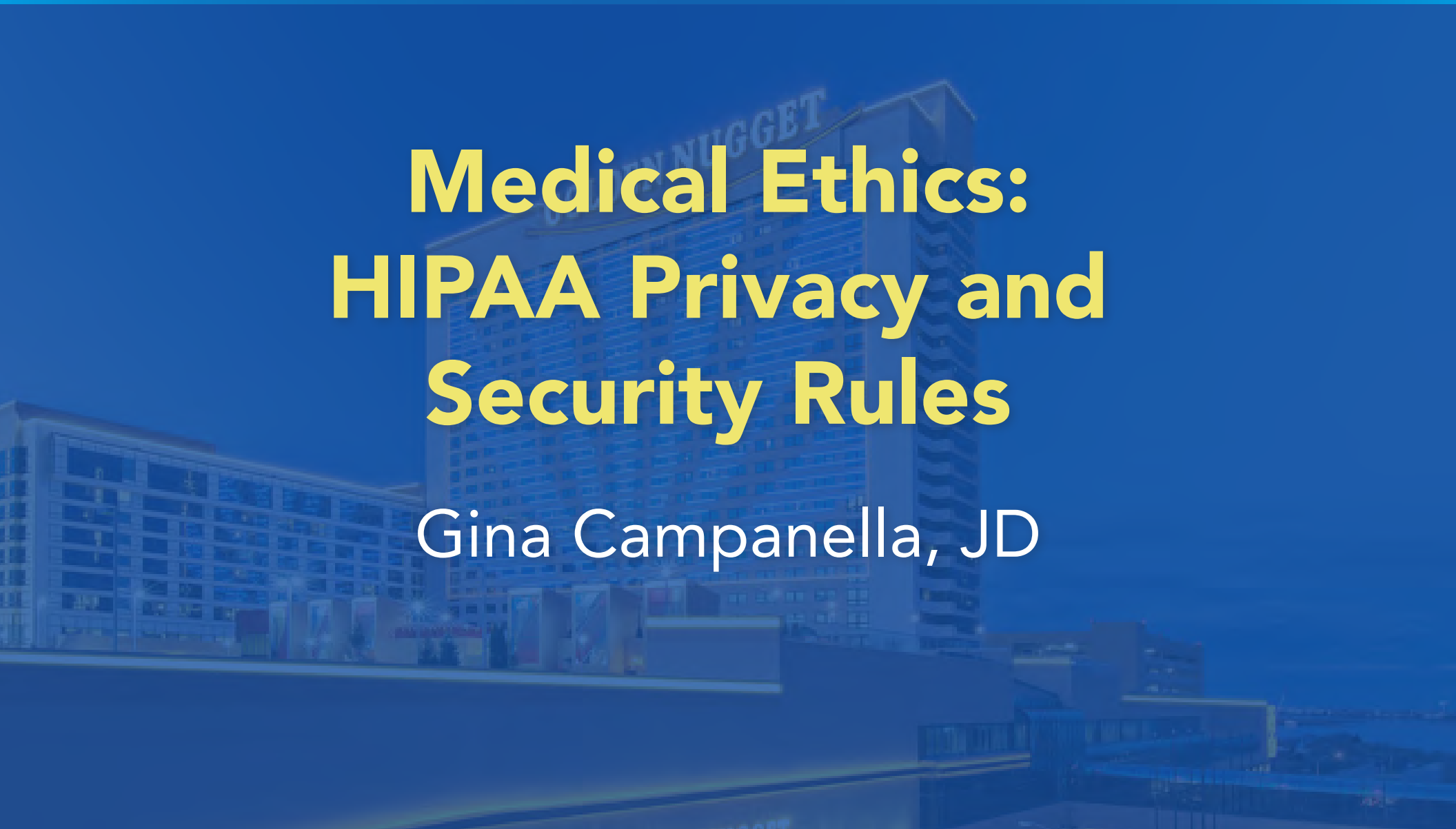
AROC 2018

Saturday, April 28



Medical Ethics: HIPAA Privacy and Security Rules

Gina Campanella, JD

HIPAA & The Medical Practice

Requirements for Privacy, Security and Breach Notification

GALLAGHER CAMPANELLA LLC
Comprehensive Care For Your Medical Practice

Gina L. Campanella, Esq. FACHE
Partner, Gallagher Campanella LLC

Speaker Background

Ms. Campanella is a founding Partner of the Gallagher Campanella LLC law firm where she focuses her practice on healthcare regulatory and transactional matters federally and in New Jersey, New York and Pennsylvania.

Ms. Campanella has assisted clients with transactional services and regulatory compliance consulting, as well as general counsel services to small practices and large societies and medical groups alike. Clients also seek her expertise when reviewing employment agreements, formation of new practices, separation from and sale of practices, business structuring, and surgical center licensing and registration.

NO Conflicts of

Rules that Control Privacy

A collection of laws and regulations including:

- The Health Insurance Portability and Accountability Act of 1996 ("HIPAA")
- Health Information Technology for Economic and Clinical Health Act of 2009 ("HITECH")
  - Privacy Rule (found at 45 C.F.R. 164.500 et. seq.)
  - Security Rule (found at 45 C.F.R. 164.300 et. seq.)
- Breach Notification Rule (found at 45 C.F.R. 164.400 et. seq.)

HIPAA

- The Health Insurance Portability and Accountability Act of 1996
  - Passed by Congress in order to require the Department of Health and Human Services (HHS) to develop national rules for the protection of electronic healthcare information.
  - Mandated that states adopt these federal protections.

HI-TECH

- Health Information Technology for Economic and Clinical Health Act of 2009
  - Adopted as part of the American Recovery and Reinvestment Act.
  - Intended to promote the adoption of and meaningful use of electronic medical records.
  - Addresses and strengthens penalties for violation of HIPAA protections of electronic health information.

Privacy, Security & Breach Notification Rules

- Privacy Rule: Establishes the set of national standards for the protection of health information.
- Security Rule: Establishes the set of national standards for the protection of health information that is electronically stored and/or transmitted.
- Breach Notification Rule: Establishes the set of national notification requirements if a Covered Entity discovers a breach of unsecured protected health information.

The Omnibus Rule

- The Privacy, Security and Breach Notification Rules were amended and combined in 2013 into what is known as the

HIPAA Privacy, Security, Enforcement and Breach Notification: Final Omnibus Rule

Changes Under the Omnibus Rule

- Notice of Privacy Practices Changes:
  - New explanatory statements to patients required (i.e. sale of PHI, marketing use of PHI and research use of PHI)
  - Must have been done on or before September 23, 2013.
- Definition of Business Associate has changed; new category of "Subcontractor Business Associate" addresses handling of PHI further downstream
  - A "grandfathered Business Associate Agreement could remain in place until September 2014; all other Business Associate Agreements needed to be revised on or before September 23, 2013
  - A "grandfathered" Business Associate Agreement is one that in place prior to January 23, 2013.

Changes Under the Omnibus Rule

- Enhanced penalties for violations
- "Breach" redefined to include presumption that an impermissible use or disclosure is a Breach
- The previously used "harm" analysis to determine if an unauthorized use or disclosure is, in fact, a breach has been replaced with a four-factor Risk Assessment
- Prohibitions on health plans using or disclosing genetic information for underwriting purposes (required by the Genetic Information Non-discrimination Act ("GINA"))
- Separate Authorizations Required for different kinds of PHI

Basic Requirements Under HIPAA

1. Notice of Privacy Practices
2. Uses and Disclosures of Protected Health Information
   a. When is patient authorization required? Not required?
3. Privacy Officer
4. Patient Access to Protected Health Information
   a. Accounting of Disclosures
   b. Amendment
5. Administrative, Technical and Physical Safeguards
6. Business Associates

Notice of Privacy Practices

All Covered Entities must have a written Notice of Privacy Practices which explains, in detail, to the patient:

- how the Covered Entity may use and/or disclose the patients protected health information,
- the patients rights as to his or her protected health information, and
- the Covered Entity's obligations as to the patient's protected health information.

Notice of Privacy Practices

The Notice of Privacy Practices must be:

- Provided to each patient upon their first visit. The patient must sign an acknowledgement that he or she received the notice and a copy of the notice received should be included in the patient's chart. If the patient refuses to sign an acknowledgement, the Covered Entity should make note of the refusal in the patient record and that the patient was provided a copy even though he or she refused to sign.
- Posted in the Covered Entity's office in an area where patients have access (i.e. the waiting room).
- Included on a Covered Entity's web site if a site is maintained.

Notice of Privacy Practices

The Notice of Privacy Practices must be:

- Provided in hard copy to any patient who asks for a copy even if it is available online or has already been provided.
- Include an effective date.

When a Covered Entity updates its Notice of Privacy Practices, it is **not** required to redistribute to every patient and obtain a new acknowledgment of receipt; however, the updated policy must be posted immediately in the office and on the web site (as applicable), reflecting the updated effective date, and must be available in hard copy for any patient who requests it.

Uses and Disclosures of PHI

- The three types of written patient Authorization for Use and Disclosure:
  - General Authorization for Use and Disclosure
  - Authorization for Use and Disclosure of Psychotherapy Notes
    - Psychotherapy notes must always be segregated from the rest of a medical record and always require a separate, specific authorization.
  - Authorization for Use and Disclosure for Marketing Purposes
    - A communication about a product or service that encourages purchase of the product or service.
      - Specifically excludes; refill reminders for prescribed medications (so long as there is no remuneration in excess of the reasonable cost of making such communications), and certain other communications for treatment and health care operations purposes where there is no remuneration to the practice in exchange for making such communications.

Uses and Disclosures of PHI

A valid authorization must be written in plain language that the typical patient can read and understand.

- What must a valid authorization contain?
  - Meaningful description of the information to be used or disclosed
  - Name or other specific identification of the person or entity authorized to make the requested use or disclosure
  - Name or other specific identification of the person or entity to whom the disclosure will be made
  - A description of purpose ("at the request of the individual" is sufficient if the patient elects not to make a specific disclosure of purpose
  - Expiration date or event
  - Signature of requesting individual

Uses and Disclosures of PHI

- Required Statements:
  - The right to revoke the authorization in writing and any exceptions to this right
  - Ability or inability to condition treatment, payment, enrollment or eligibility for benefits on the authorization
    - Consequences of refusal to sign when there is a lawful ability to condition treatment, payment, enrollment or eligibility for benefits on the authorization
  - The potential that information disclosed pursuant to the authorization may be subject to re-disclosure by the recipient and any disclosures made prior to a revocation will not eradicate any disclosures already made.

Uses and Disclosures of PHI

- When is a written authorization required?
  - When the disclosure is for any reason other than the:
    - Treatment
    - Payment
    - Health care operations
  - When the disclosure is not one that is otherwise permitted under HIPAA.

Uses and Disclosures of PHI

- When is oral authorization sufficient?
  - Informal permission, or "the opportunity to agree or object" is sufficient to allow disclosures in the following circumstances:
    - Facility directory of patient contact information.
    - Notification or disclosure to family, friends or relatives only to the extent that person is involved in the patient's care and/or payment for the patient's care.
    - Notification to a school regarding a students immunization records.

Uses and Disclosures of PHI

- When is authorization not required?
  - For the Public Interest and Benefit. Specifically:
    - Required by law (gunshot wound in the ER)
    - Public Health Activities (CDC, OSHA, FDA, etc.)
    - Victims of Abuse, Neglect or Domestic Violence
    - Health Oversight Activities (Joint Commission, DHSS)
    - Judicial and Administrative Proceedings (remember: only if there is a COURT ORDER. Subpoena is not sufficient without more!)
    - Law Enforcement Purposes (locate a suspect, info about victim, if there is suspicion of a crime that caused injury or death, medical emergency)
    - Decedents (funeral directors, medical examiners)

Uses and Disclosures of PHI

- When is authorization not required?
  - For the Public Interest and Benefit. Specifically:
    - Organ donation
    - Research (only with IRB approval)
    - Serious Threat to Health or Safety (credible threats, involuntary behavior)
    - Essential Government Functions (military, inmates, determinations of eligibility for federal benefits)
    - Workers' Compensation

Practice Privacy Officer

- All practices should have one individual who is the designated Privacy Officer. It is this individual's responsibility to make sure that the practice meets all requirements of HIPAA. The Privacy Officer should:
  - Perform regular internal Compliance Risk Assessment reviews
  - Conduct regular staff training on the requirements and implementation of HIPAA

Administrative Safeguards

- **Security Processes** – electronic security measures must be implemented that reduce risk and vulnerabilities to ePHI.
- **Security Official** – a person or persons must be designated to oversee the implementation and enforcement of these policies.
- **Information Access** – individuals should not be permitted to access information that they do not need to perform their job. There should be measures in place to prevent and trace access.
- **Training** – training, supervision and sanctions (when appropriate) for workforce members are all required.
- **Evaluation** – periodic evaluation of all of the above is required.

Technical Safeguards

- **Access control** – passwords/logins only for those who need access.
- **Audit control** – hardware, software and/or procedural mechanisms that track access control.
- **Integrity controls** – procedures to ensure that ePHI is not impermissibly altered or destroyed.
- **Transmission security** – policies to ensure that ePHI cannot be intercepted while being transmitted electronically
  - Encryption is the best way to do this – but is not required.

Physical Safeguards

- **Facility access and control** – door locks, access cards, alarm systems, no unauthorized persons, etc.
- **Workstation and device security** – laptop/desktop locks, policies regarding use of laptops off site, policies and procedures for disposal of old technology, remote "wiping" services for smartphones, tablets, etc.

Has There Been A Breach?

- The Covered Entity must first conduct an assessment to determine if the questioned event is a breach. At least the following must be considered:
  - Nature and extent of the PHI involved' likelihood of identification
  - The unauthorized person or persons who received or accessed the PHI
  - Whether the PHI actually acquired or viewed
  - The extent to which the risk has been mitigated
- If the Covered Entity determines that the incident or event is a breach – they must notify the individuals, the Secretary and, in some cases, the media.

Has There Been A Breach?

- All Breaches:
  - Notification to the individuals within 60 days of discovery by first class mail. If the entity has insufficient contact information for 10 or more individuals, the entity must post notice of the breach on its website or in a local newspaper with a toll free number where individuals can call to find out if they were effected. The number must remain active for a minimum of 90 days.
- Fewer than 500 individuals effected:
  - Notification to Secretary required within 60 days of the end of the calendar year in which the breach is *discovered*
- More than 500 individuals effected:
  - Notification to the Secretary required "without unreasonable delay" but no later than 60 days after the date of discovery.
  - Notification to the media is required.

Business Associates

- Who is a Covered Entity?
  - Any provider that transmits any information in electronic form (doctors, clinics, hospitals, surgical centers, psychologists, dentists, chiropractors, nursing homes, assisted living, pharmacies, etc.)
  - Health plans (private and government insurance, HMOs)
  - Health care clearinghouse
- Who is a Business Associate?
  - Any person or entity, other than a member of the Covered Entity's workforce, who performs services for or on behalf of the Covered Entity that involves access to protected health information. **Includes subcontractors of business associates**.
- Who is NOT a Business Associate?
  - Any person or entity who provides services to the Covered Entity that

    does not involve access to protected health information.

usiness Associate Agreements

- A written agreement between the Covered Entity and the Business Associate or between the Business Associate and their Subcontractor that:
  - Establishes permissible use and disclosure of the protected health information by the Business Associate
  - Provides that the Business Associate will not further disclose the protected health information or use it in any way not permitted by the agreement or by law
  - Requires the Business Associate to implement the same HIPAA Security Rule safeguards as the Covered Entity
  - Requires the Business Associate to disclose protected health information as needed by the Covered Entity to respond appropriately to disclosure requests.

usiness Associate Agreements

- A written agreement between the Covered Entity and the Business Associate or between the Business Associate and their Subcontractor that:
  - Requires the Business Associate to abide by the HIPAA Privacy Rule, as applicable
  - Requires the Business Associate to make all records available to the Department of Health and Human Services should the Covered Entity be required to produce same
  - Require Business Associate to return, destroy or continue to securely store all protected health information upon termination of the service agreement
  - Authorize the Covered Entity to immediately terminate the agreement should the Business Associate or a Subcontractor violates a material term.

Business Associate Subcontractors

Business Associates are required to have similar agreements with their Subcontractors. Such a requirement should be included as a term of the Business Associate Agreement.

- Who is a Business Associate Subcontractor?
  - Same analysis to determine if a person or entity is a Business Associate applies to determination of whether a person or entity is a Business Associate Subcontractor:
    - Any person or entity, other than a member of the Business Associate's workforce, who performs services for or on behalf of the Business Associate that involves access to protected health information.

Business Associate Subcontractor Agreements

- Business Associate's will typically be required, within the terms of their Business Associate Agreement, to have a similar written agreement with any Subcontractor they utilize.
- These agreements should contain all of the same obligations of the Business Associate Subcontractor to the Business Associate as the Business Associate is obligated to the Covered Entity.

Enforcement Actions

- The federal Office for Civil Rights ("OCR") has the duty and responsibility to investigate complaints or reports of potential HIPAA violations and to continuously monitor entities required to comply with HIPAA ("Covered Entities") for compliance.
- OCR began a preliminary pilot program for random compliance audits of Covered Entities in 2015.

Enforcement Actions

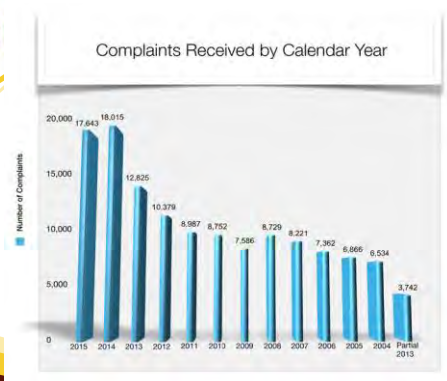
- The OCR looks at several areas of HIPAA compliance when performing an audit including:
  - Does the Covered Entity have a Notice of Privacy Practices? Is the notice complete? Is the notice posted and distributed properly?
  - What are the patients' rights to request privacy protections, access to or an accounting of disclosures of their protected heath information ("PHI")?

Enforcement Actions

- The OCR looks at several areas of HIPAA compliance when performing an audit including:
  - What are the Covered Entities administrative requirements for the security of PHI?
  - Does the Covered Entity have proper Authorizations for Use and Disclosure of PHI available for patient use?
  - Are there proper administrative, physical and technical safeguards in place on the premises of the Covered Entity?

Enforcement Actions

- OCR was on schedule to begin its second round of HIPAA audits in early 2016 and plans to include many more types of Covered Entities than were included in the first phase as well as Business Associates (as defined by HIPAA) of Covered Entities.
- One of the essential items that OCR will be looking for is the proper performance of an internal Compliance Risk Assessment and the implementation of any necessary plans to cure any problems that are discovered as a result of the Compliance Risk Assessment.



https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/complaints-received-by-calendar-year/index.html

Top Five Issues in Investigated Cases Closed with Corrective Action, by Calendar Year

Year	Issue 1	Issue 2	Issue 3	Issue 4	Issue 5
2015	Impermissible Uses & Disclosures	Safeguards	Administrative Safeguards	Access	Technical Safeguards
2014	Impermissible Uses & Disclosures	Safeguards	Administrative Safeguards	Access	Technical Safegards
2013	Impermissible Uses & Disclosures	Safeguards	Access	Administrative Safeguards	Minimum Necessary
2012	Impermissible Uses & Disclosures	Safeguards	Administrative Safeguards	Access	Minimum Necessary

https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/data/complaints-received-by-calendar-year/index.html

Questions?

GALLAGHER CAMPANELLA LLC
Comprehensive Care For Your Medical Practice

356 Franklin Avenue, 2nd Floor * Wyckoff, NJ 07481
52 Elm Street, Suite 1, Morristown, NJ 07960
(201) 891-3726 * (973) 998-8494
Gina@GCHealthLaw.com

GCHealthLaw.com