SUMMARY OF THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (HIPAA)

A. BACKGROUND

I. What is HIPAA?

The Health Insurance Portability and Accountability Act of 1996 ("HIPAA") was enacted, in part, to protect the privacy of health information. It was intended to provide individuals with at least a minimum level of privacy and security for their health information although state laws may provide additional protections for such information. HIPAA applies to health information that is defined as "protected health information" ("PHI") under HIPAA.

II. What is PHI?

In general, HIPAA defines PHI to comprise all of the following four elements:

1. **Health information** (whether oral or recorded in any form or medium), including demographic information collected from an individual, that is created or received by a health care provider, health plan, employer or health care clearinghouse that

2. **transmitted or maintained** in electronic media or in any other form or medium, and

3. **relates to**: (i) the past, present, or future physical or mental health or condition of an individual, (ii) the provision of health care to an individual, or (iii) the past, present, or future payment for the provision of health care to an individual, and

4. **reasonably identifies** the individual.

HIPAA's privacy rules do not apply to health information that has been "de-identified" in accordance with HIPAA's de-identification regulations. In general, to de-identify health information a covered entity must use the services of a qualified statistician or must otherwise remove numerous types of identifiers from the data to ensure that there is no possibility of re-identifying the individuals associated with it.

III. Who is Covered By HIPAA?

In general, most of HIPAA's privacy provisions apply to both "covered entities" and "business associates". As of September 23, 2013, HIPAA's security rules will apply to business associates in addition to covered entities, which are already subject to the HIPAA security rules. Covered entities include health plans, health care clearinghouses, and health care providers such as optometry practices that transmit any health information in electronic form in connection with a covered transaction (e.g., electronically billing a health care payer). Business associates are those entities that create, receive, maintain or transmit PHI on behalf of a covered entity for a covered function, including for things like claims processing, data analysis, processing, administration, quality assurance, utilization review, benefit or practice management, billing or safety
activities. Business associates are also defined to include subcontractors that create, receive, maintain or transmit PHI on behalf of other business associates.

Covered entities may constitute business associates of one another under some circumstances. However, disclosures by a covered entity to another health care provider do not render the provider a business associate of the disclosing entity if the disclosure is related to the treatment of an individual. For instance, a disclosure of PHI made by an optometrist to another health care provider who is consulting on the patient's treatment would not render the receiving provider a "business associate" of the optometrist solely by reason of that disclosure.

B. THE PRIVACY RULE

IV. What Do HIPAA's Privacy Rules Require?

HIPAA's privacy rules prohibit a covered entity from disclosing PHI for purposes unrelated to payment, treatment or health care operations unless the individual's authorization is first obtained. Any authorization must be in writing and must meet the form and content requirements of the HIPAA regulations. HIPAA also contains certain exceptions that allow covered entities to disclose PHI without the individual's authorization or consent for certain events or purposes (e.g., emergencies, public health, administration of workers compensation claims). HIPAA also requires that when a covered entity uses or discloses PHI it must limit such information to the "minimum necessary" to achieve the intended purpose of the use or disclosure. Covered entities must also make a "Notice of Privacy Practices" available to individuals that discloses when and how the covered entity can disclose PHI and the individual's rights with respect to his or her PHI. Contact AOA for a form of Notice of Privacy Practices that can be adapted for your practice's particular needs.

V. What are Some Rights that Individuals Have with Respect to their PHI?

HIPAA grants individuals several rights in connection with their PHI. In general, these include:

- Access to the individual's PHI;
- Amendment of the individual's PHI;
- Accounting of the covered entity's past disclosures of the individual's PHI;
- Ability to restrict disclosures of the individual's PHI under certain circumstances;
- Permission to allow an individual's personal representatives access to his or her PHI; and
- Ability to revoke an individual's authorization to disclose or use his or her PHI.

C. THE SECURITY RULE

VI. What is the HIPAA Security Rule/Security Regulation?

While the HIPAA privacy rules deal with any PHI (whether written or oral), the HIPAA security rules governs electronic PHI ("ePHI"). The security rule requires covered entities – and, as of September 23, 2013, business associates – to implement three types of safeguards with respect to ePHI: (1) administrative; (2) physical; and (3) technical. These are highly technical requirements that are essentially a compilation of best practices in the industry with respect to the protection of electronic data. HIPAA requires all covered entities and business associates, large and small, to "reasonably and appropriately" comply with these standards. HIPAA also imposes requirements on covered entities and business associates to implement policies and procedures with respect to compliance with the security rules as well as certain documentation requirements.
These entities must also appoint a "security officer" and train their workforce members on the entity's ePHI security protocols. For more information about the HIPAA Security Regulation, see the AOA's HIPAA Security Regulation Compliance Manual.

D. BREACH NOTIFICATION

VII. What Must a Covered Entity Do if there is a Breach of Unsecured PHI?

Following the discovery of a breach of unsecured PHI, a covered entity must notify each individual whose unsecured PHI was, or was reasonably believed to have been, accessed, acquired, used or disclosed as a result of the breach. The notification must be made "without unreasonable delay" and in no event later than 60 calendar days after discovery of the breach. The notice must be in writing and must conform to the form and content requirements of the HIPAA regulations. The covered entity must also report the breach to the Secretary of Health and Human Services ("HHS") using HHS's online filing procedures. The manner and form of the notification to HHS depends on the number of individuals whose PHI was breached. More prompt and comprehensive notification is required for breaches involving more than 500 individuals. HHS also has authority to impose civil money penalties on a covered entity for a breach of PHI or for other technical violations of HIPAA requirements. HIPAA further requires a business associate of a covered entity to notify the covered entity of the business associate's breach of unsecured PHI without unreasonable delay and in no event later than 60 days after the business associate's discovery of the breach.

VIII. When is there a "Breach" of Unsecured PHI?

Under the HIPAA Final Rule effective for covered entities and business associates on September 23, 2013, all non-permitted acquisitions, accesses, uses or disclosures of PHI which compromise the security or privacy of the PHI are presumed to constitute a breach. In determining whether a covered entity can overcome the presumption of a breach, the Final Rule requires covered entities to undergo a "risk assessment" based on several factors to determine whether there was a low probability that the PHI was compromised by the non-permitted acquisition, access, use or disclosure. Those factors include the following:

1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
2. The unauthorized person who used the PHI or to whom the disclosure was made;
3. Whether the PHI was actually acquired or viewed; and
4. The extent to which the risk to the PHI has been mitigated.

E. MORE INFORMATION

Contact HHS or your health care attorney for more information or resources about HIPAA compliance. HHS's HIPAA website can be viewed here: http://www.hhs.gov/ocr/privacy/.