ALFA INTERNATIONAL
2015 INSURANCE LAW SEMINAR
June 10-12, 2015 – The Ritz-Carlton Battery Park –
New York, New York

KEEPING OFF THE ROCKS:
HIPAA PRIVACY RULE, BUSINESS ASSOCIATE AGREEMENTS, COMPLIANCE ISSUES AND TRENDS

Careen Martin
Moderator
NILAN JOHNSON LEWIS, PA
Minneapolis, Minnesota
cmartin@nilanjohnson.com
I. BACKGROUND

The Health Insurance Portability and Accountability Act (HIPAA), enacted in 1996, was intended to improve the efficiency and effectiveness of the health care system in the United States. The Administrative Simplification provisions of HIPAA were added to improve the Medicare and Medicaid programs and to promote the efficiency of the health care system by creating national standards and requirements for the electronic transmission of health information. The Administrative Simplification provisions required the Department of Health and Human Services (HHS) to adopt standards for the electronic transmission of health care transactions, and to protect the confidentiality, integrity, and security of personal health information. Accordingly, HHS has issued three sets of federal regulations: (1) Transactions and Code Set Standards; (2) Privacy Rule; and (3) Security Rule.

II. WHAT INFORMATION IS PROTECTED

The HIPAA Privacy Rule protects all “individually identifiable health information” held or transmitted by a Covered Entity or its Business Associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information “protected health information (PHI).” “Individually identifiable health information” is information, including demographic data, that relates to:

- the individual’s past, present or future physical or mental health or condition,
- the provision of health care to the individual, or
- the past, present, or future payment for the provision of health care to the individual,
- and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual.

Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number). The Privacy Rule excludes certain information from the definition of PHI, including employment records that a covered entity maintains in its capacity as an employer and education records.

Under HIPAA there are no restrictions on the use or disclosure of de-identified health information. De-identified health information neither identifies nor provides a reasonable basis

---

1 42 U.S.C. § 1320d et seq.
3 45 C.F.R. § 160.103.
4 Id.
5 Id.
6 Id.
7 45 C.F.R. § 164.514(c)
to identify an individual. To fall under the de-identified safe harbor, the following eighteen identifiers must be removed:

- Names
- All geographic subdivisions smaller than a state, including street address, city, county, precinct, ZIP code
- All elements of dates (except year) for dates that are directly related to an individual, including birth date, admission date, discharge date, death date, and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older
- Telephone numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Fax numbers
- Device identifiers and serial numbers
- Email addresses
- Web Universal Resource Locators (URLs)
- Social security numbers
- Internet Protocol (IP) addresses
- Medical record numbers
- Biometric identifiers, including finger and voice prints
- Health plan beneficiary numbers
- Full-face photographs and any comparable images
- Account numbers
- Any other unique identifying number, characteristic, or code

The removal of specified identifiers of the individual and of the individual’s relatives, household members, and employers is required, and is adequate only if the Covered Entity has no actual knowledge that the remaining information could be used to identify the individual.15

III. TO WHOM DOES HIPAA APPLY

HIPAA originally applied to “Covered Entities,” defined as (1) health plans; (2) health care clearinghouses; and (3) health care providers that transmit any health information in electronic
form in connection with a transaction covered by HIPAA. However, due to recent changes, Business Associates of Covered Entities are also now directly liable for violation of certain provisions of the HIPAA Privacy Rule and Security Rule.

A. Health Plans

The definition of Covered Entity under HIPAA includes “health plans.” A health plan is an individual or group plan that provides or pays the cost of medical care. Specifically, health plan includes: a health insurance issuer; an HMO; Part A or Part B of the Medicare program; Medicaid; Prescription Drug Benefit Program; Medicare supplemental; an issuer of a long-term care policy, excluding a nursing home fixed indemnity policy; an employee welfare benefit plan or any other arrangement that is established or maintained for the purpose of offering or providing health benefits to the employees of two or more employers; the health care program for uniformed services; the veterans’ health care program; the Indian Health Service program; the Federal Employees Health Benefits Program; an approved State child health plan; Medicare Advantage; a high risk pool that is a mechanism established under State law to provide health insurance coverage or comparable coverage to eligible individuals; any other individual or group plan, or combination of individual or group plans, that provides or pays for the cost of medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg-91(a)(2)).

The definition of “health plan” for purposes of HIPAA excludes any policy, plan, or program to the extent that it provides, or pays for the cost of, excepted benefits. Excepted benefits are one or more (or any combination thereof) of the following policies, plans or programs: coverage only for accident or disability income insurance, or any combination thereof; coverage issued as a supplement to liability insurance; liability insurance, including general liability insurance and automobile liability insurance; workers’ compensation or similar insurance; automobile medical payment insurance; credit-only insurance; coverage for on-site medical clinics; other similar insurance coverage, specified in regulations, under which benefits for medical care are secondary or incidental to other insurance benefits.

Therefore, the HIPAA regulations are generally not applicable to disability insurance carriers or worker’s compensation carriers.

B. Health Care Providers

A Covered Entity under HIPAA includes “health care providers.” Health care provider means a provider of services, a provider of medical or health services (as defined in section 1861(s) of the Act, 42 U.S.C. 1395x(s)), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business. The term “provider of services” means a hospital, critical access hospital, skilled nursing facility, comprehensive outpatient rehabilitation facility, home health agency, hospice program, or, for purposes of section 1814(g) and section 1835(e), a fund. “Health care” means care, services, or supplies related to the health of an individual,

---

8 45 C.F.R. §160.103.
9 45 C.F.R. § 160.103.
10 Public Health Service Act, 42 U.S.C. 300gg-91(c)(1); see 45 CFR 160.103.
11 42 U.S.C. 1395x(s)(2)(m).
12 42 U.S.C. 1395x(u).
including (1) preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and (2) sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.\(^{13}\)

As discussed below, where an entity meets the definition of health care provider, to qualify as a Covered Entity, the entity must also transmit health information in electronic form, in connection with a transaction covered by HIPAA.

1. **Covered Transactions**

Covered Entities include health care providers that transmit any health information in electronic form in connection with a transaction covered by HIPAA.\(^{14}\) For purposes of determining whether a transaction is “covered” by HIPAA, “transaction” means “the transmission of information between two parties to carry out financial or administrative activities related to health care.”\(^{15}\) Specifically, it includes the following types of information transmissions:

1. Health care claims or equivalent encounter information, including a request to obtain payment or, if there is no direct claim because the reimbursement contract is based on a mechanism other than charges or reimbursement rates for specific services, the transaction is the transmission of encounter information for the purpose of reporting health care
2. Health care payment and remittance advice, including transmission of payment, information about the transfer of funds, payment processing information, and explanation of benefits
3. Coordination of benefits
4. Health care claim status
5. Enrollment and disenrollment in a health plan
6. Eligibility for a health plan, including an inquiry from a health care provider to a health plan to obtain coverage information
7. Health plan premium payments
8. Referral certification and authorization, including a request for the review of health care to obtain an authorization for health care or a request to obtain authorization for referring an individual to another health care provider.
9. First report of injury
10. Health claims attachments\(^{16}\)

Whether an organization will be considered a Covered Entity subject to HIPAA depends on whether it is engaging in any of the covered transactions listed above.

2. **Electronic Form**

\(^{13}\) 45 C.F.R. § 160.103.
\(^{14}\) 45 C.F.R. §160.104(a).
\(^{15}\) 45 C.F.R. §160.103.
\(^{16}\) 45 C.F.R. §160.103; 45 C.F.R. Part 162, subparts k-r.
The final question in the Covered Entity analysis is whether the organization transmits any health information related to such covered transactions in electronic form. A Covered Entity includes health care providers who transmit any health information in electronic form in connection with a transaction covered by HIPAA. The term “in electronic form” means using electronic media, electronic storage media (e.g. hard/floppy disk, hard drive) including memory devices in computers (hard drives), and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card. Transmission media includes Internet and Intranet. Telephone and faxes are not considered electronic media.

If any of the organization’s services are “covered” services under the categories defined above, and the organization uses any electronic transmission process, then it is a Covered Entity subject to HIPAA.

C. Health Care Clearinghouse

A Covered Entity under HIPAA includes “health care clearinghouse.” Health care clearinghouse means a public or private entity, including a billing service, repricing company, community health management information system or community health information system, and “value-added” networks and switches, that does either of the following functions: (1) processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into a standard transaction; or (2) receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.

D. Business Associates

The HIPAA Privacy Rule applies only to covered entities – health plans, health care clearinghouses, and certain health care providers. However, most health care providers and health plans do not carry out all of their health care activities by themselves. Instead, they use the services of a variety of other businesses or contractors. To address this, the Privacy Rule allows Covered Entities to disclose PHI to these “business associates” with certain written assurances, which are outlined in a Business Associate Agreement. Specifically, the Covered Entity must obtain satisfactory assurances that the Business Associate will use the information only for the purposes for which it was engaged by the Covered Entity; will safeguard the information from misuse; and will help the Covered Entity comply with some of the covered entity’s duties under the Privacy Rule. Covered Entities may disclose PHI to an entity in its role as a Business Associate only to help the Covered Entity carry out its health care functions – not for the Business Associate’s independent use or purposes, except as needed for the proper management and administration of the Business Associate.

1. Who is a Business Associate

A “business associate” is a person or entity that performs certain functions or activities that involve the use or disclosure of PHI on behalf of, or provides services to, a covered

---

17 45 C.F.R. §§ 164.103, 165.502(e), and 164.504(e).
18 Id.
entity. Business Associate functions and activities include: claims processing or administration; data analysis, processing or administration; utilization review; quality assurance; billing; benefit management; practice management; and repricing. Business Associate services include legal; actuarial; accounting; consulting; data aggregation; management; administrative; accreditation; and financial.

Examples of Business Associates include:

- A third party administrator that assists a health plan with claims processing.
- A CPA firm whose accounting services to a health care provider involves access to PHI.
- An attorney whose legal services to a health plan involves access to PHI.
- A consultant that performs utilization reviews for a hospital.
- A health care clearinghouse that translates a claim from a non-standard format into a standard transaction on behalf of a health care provider and forwards the processed transaction to a payer.
- An independent medical transcriptionist that provides transcription services to a physician.
- A pharmacy benefits manager that manages a health plan’s pharmacist network.

2. Business Associate Obligations

Regardless of the provisions in a Business Associate Agreement, Business Associates have direct liability under HIPAA for the following:

- Uses and disclosures of PHI, except those permitted or required by the business associate agreement or as required by law;
- Uses and disclosures of PHI that would violate the Privacy Rule if done by the Covered Entity (except for certain permitted uses and disclosures of PHI for the proper management and administration of the business associate, or to provide certain data aggregation services for the covered entity);
- Failure to provide a required breach notification to the covered entity;
- Failure to provide access to a copy of electronically maintained PHI requested by an individual (to be provided to the Covered Entity in accordance with the Business Associate Agreement);
- Failure to disclose PHI when required by HHS;

19 45 C.F.R. § 160.103.
20 Id.
21 Id.
22 http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.html
23 45 C.F.R. § 164.502(a)(3).
24 45 C.F.R. § 164.502(a)(3).
25 45 C.F.R. § 164.410(a).
• Failure to take reasonable steps to cure a breach or end a violation if the business associate knows of a pattern or practice that is a material breach of the business associate agreement;\textsuperscript{28}
• Failure to provide an accounting of disclosures;\textsuperscript{29}
• Failure to comply with the Security Rule.\textsuperscript{30}

3. **Business Associate Agreement**

A Covered Entity’s contract or other written arrangement with its Business Associate must contain the elements specified in the Privacy Rule.\textsuperscript{31} Many organizations have expanded Business Associate Agreements to contain additional provisions, such as indemnification. These provisions are not required under HIPAA, and are therefore a matter of contract negotiation. To comply with HIPAA, a Business Associate Agreement must:

- Describe the permitted and required uses of PHI by the Business Associate;
- Provide that the Business Associate will not use or further disclose the PHI other than as permitted or required by the contract or as required by law;
- Require the Business Associate to use appropriate safeguards to prevent a use or disclosure of the PHI other than as provided for by the contract.
- Require the Business Associate to report any unauthorized use or disclosure, security incident, or Breach to the Covered Entity;
- Prohibit the Business Associate from doing anything that would violate HIPAA if done by the Covered Entity;
- Ensure that any agent, including a subcontractor, to whom the Business Associate provides such information agrees to the same restrictions and conditions that apply to the Business Associate;
- Honor individuals’ rights under HIPAA, including access, amendment, and accounting of disclosures;
- Make available to HHS the Business Associate’s internal practices, books, and records relating to the use and disclosure of PHI received from or created on behalf of the Covered Entity for purposes of determining the Covered Entity’s compliance with HIPAA;
- Authorize termination of the contract if the Covered Entity determines that the Business Associate has violated a material term of the contract; and
- Return to the Covered Entity, or destroy all PHI at the termination of the contract so that the Business Associate maintains no copies of the information in any form. If return or

\textsuperscript{27} 45 C.F.R. § 164.502(a)(4)(i).
\textsuperscript{28} 45 C.F.R. § 164.502(e)(1)(iii).
\textsuperscript{29} HITECH Act § 13405.
\textsuperscript{30} HITECH Act § 13401(a).
\textsuperscript{31} 45 CFR 164.504(e)
destruction is not feasible, extend the protections of the contract to the retained information.\textsuperscript{32}

II. LAWYERS AS BUSINESS ASSOCIATES

Clients may ask their lawyer to sign a Business Associate Agreement as a matter of course. As a matter of good business practice, the lawyer may agree to sign the Business Associate Agreement without conducting an analysis as to whether a Business Associate Agreement is truly required. However, it is worth noting that lawyers are not always Business Associates. To determine whether a lawyer is a Business Associate, there are three key questions:

1. Is the client a Covered Entity (or the Business Associate of a Covered Entity)?
2. If the client is a Covered Entity, is the lawyer obtaining, creating, using, or disclosing the client’s PHI?
3. Is the PHI required or related to the specific representation?

If the answer to all three questions is “yes,” then the lawyer is a Business Associate. For example, a lawyer is a Business Associate under the following circumstances:

- Lawyer represents a health plan in the acquisition of another plan and reviews individually identifiable member data as part of the due diligence.
  - The health plan is a Covered Entity, the health plan is providing its member PHI, and the PHI is being provided to the attorney relative to the due diligence.

- Lawyer appeals a large hospital’s Medicare denials and receives patient records.
  - The hospital is a Covered Entity, the hospital’s patient’s PHI is provided to the lawyer, and the lawyer is using the PHI for the Medicare appeal.

- Lawyer defends self-insured employer health plan in litigation and requires member plan data.
  - The health plan is a Covered Entity, the lawyer receives the member’s plan information, and the representation is for purposes of the litigation.

For other types of representation, the lawyer may not be a Business Associate. For example, a lawyer is not a business associate if the lawyer is defending a drug manufacturer in a products liability case and receives the plaintiff’s medical records in discovery. Even if the client drug manufacturer is a Covered Entity, the lawyer is not using the manufacturer’s PHI to provide legal services; rather the medical records are coming from the Plaintiff. Similarly, a lawyer would not be a business associate if the lawyer is defending an employment discrimination claim against a hospital and receives plaintiff’s medical records from plaintiff’s clinic and plaintiff’s employment records from the hospital.

\textsuperscript{32} 45 C.F.R. § 164.504(e)(2).
III. ENFORCEMENT TRENDS

The U.S. Department of Health and Human Services Office for Civil Rights (OCR) investigates complaints, conducts audits, and handles enforcement activities relative to HIPAA. OCR has made clear that it will continue to actively enforce HIPAA, as evidenced by recent civil monetary penalties, resolution agreements, and settlements. Recent enforcement matters tend to involve theft, incident response, risk analyses, and follow through on risk analyses.

Recent enforcement actions include:33

- A complaint alleged that an HMO impermissibly disclosed a member’s PHI, when it sent her entire medical record to a disability insurance company without her authorization. An OCR investigation indicated that the form the HMO relied on to make the disclosure was not a valid authorization under the Privacy Rule. Among other corrective actions to resolve the specific issues in the case, the HMO created a new HIPAA-compliant authorization form and implemented a new policy that directs staff to obtain patient signatures on these forms before responding to any disclosure requests, even if patients bring in their own “authorization” form. The new authorization specifies what records and/or portions of the files will be disclosed and the respective authorization will be kept in the patient’s record, together with the disclosed information.

- A municipal social service agency disclosed PHI while processing Medicaid applications by sending consolidated data to computer vendors that were not business associates. Among other corrective actions to resolve the specific issues in the case, OCR required that the social service agency develop procedures for properly disclosing PHI only to its valid business associates and to train its staff on the new processes. The new procedures were instituted in Medicaid offices and independent health care programs under the jurisdiction of the municipal social service agency.

- An HMO sent explanation of benefits (EOB) by mail to a complainant’s unauthorized family member. OCR’s investigation determined that a flaw in the health plan’s computer system put the PHI of approximately 2,000 families at risk of disclosure in violation of the Rule. Among the corrective actions required to resolve this case, OCR required the insurer to correct the flaw in its computer system, review all transactions for a six month period and correct all corrupted patient information.

- A health system agreed to settle potential violations by paying a penalty of $800,000 and adopting a corrective action plan to address deficiencies in its HIPAA compliance program. OCR opened an investigation after receiving a complaint from a retiring physician alleging that the health system had violated the HIPAA Privacy Rule. In September 2008, the health system took custody of medical records pertaining to approximately 5,000 to 8,000 patients while assisting the retiring physician to transition her patients to new providers, and while considering the possibility of purchasing some of the physician’s practice. On June 4, 2009, the health system employees, with notice that

33 http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/
the physician was not at home, left 71 cardboard boxes of these medical records unattended and accessible to unauthorized persons on the driveway of the physician’s home, within 20 feet of the public road and a short distance away from a heavily trafficked public shopping venue.

- New York Presbyterian Hospital/Columbia University Medical Center agreed to settle an OCR claim that they failed to secure thousands of patients’ electronic PHI (ePHI) held on their network. The monetary payments of $4,800,000 are the largest HIPAA settlement to date. OCR initiated its investigation of New York and Presbyterian Hospital (NYP) and Columbia University (CU) following their submission of a joint breach report regarding the disclosure of the ePHI of 6,800 individuals, including patient status, vital signs, medications, and laboratory results. The investigation revealed that the breach was caused when a physician employed by CU who developed applications for both NYP and CU attempted to deactivate a personally-owned computer server on the network containing NYP patient ePHI. Because of a lack of technical safeguards, deactivation of the server resulted in ePHI being accessible on internet search engines. The entities learned of the breach after receiving a complaint by an individual who found the ePHI of the individual’s deceased partner, a former patient of NYP, on the internet. In addition to the impermissible disclosure of ePHI on the internet, OCR’s investigation found that neither NYP nor CU made efforts prior to the breach to assure that the server was secure and that it contained appropriate software protections. Moreover, OCR determined that neither entity had conducted an accurate and thorough risk analysis that identified all systems that access NYP ePHI. As a result, neither entity had developed an adequate risk management plan that addressed the potential threats and hazards to the security of ePHI. Lastly, NYP failed to implement appropriate policies and procedures for authorizing access to its databases and failed to comply with its own policies on information access management.

- OCR opened a compliance review of a health system upon receiving a breach report that an unencrypted laptop was stolen from one of its facilities. OCR’s investigation revealed that the health system had previously recognized in multiple risk analyses that a lack of encryption on its laptops, desktop computers, medical equipment, tablets and other devices containing ePHI was a critical risk. While steps were taken to begin encryption, the health system’s efforts were incomplete and inconsistent over time leaving patient PHI vulnerable throughout the organization. OCR’s investigation further found the health system had insufficient security management processes in place to safeguard patient information. The health system agreed to pay OCR $1,725,220 to settle potential violations and will adopt a corrective action plan to evidence their remediation of these findings.

- OCR received a breach notice in February 2012 from a health plan reporting that an unencrypted laptop computer containing the ePHI of 148 individuals was stolen from a workforce member’s car. While the health plan encrypted their devices following discovery of the breach, OCR’s investigation revealed that the health plan failed to comply with multiple requirements of the HIPAA Privacy and Security Rules, beginning from the compliance date of the Security Rule in April 2005 and ending in June 2012. The health plan agreed to a $250,000 monetary settlement and is required to provide
HHS with an updated risk analysis and corresponding risk management plan that includes specific security measures to reduce the risks to and vulnerabilities of its ePHI.

- A health plan settled potential violations of HIPAA for $1,215,780. The health plan filed a breach report with OCR indicating that it was informed by a representative of CBS Evening News that, as part of an investigatory report, CBS had purchased a photocopier previously leased by the plan. CBS informed the plan that the copier contained confidential medical information on the hard drive. The plan estimated that up to 344,579 individuals may have been affected by the breach. OCR’s investigation indicated that the plan impermissibly disclosed the PHI of these affected individuals when it returned multiple photocopiers to leasing agents without erasing the data contained on the copier hard drives. In addition, the investigation revealed that the plan failed to incorporate the electronic PHI (ePHI) stored on photocopier hard drives in its analysis of risks and vulnerabilities as required by the Security Rule, and failed to implement policies and procedures when returning the photocopiers to its leasing agents.

- A managed care company paid $1.7 million for leaving information accessible over Internet. OCR began its investigation following a breach report submitted by the managed care company. The report indicated that security weaknesses in an online application database left the ePHI of 612,402 individuals accessible to unauthorized individuals over the Internet. OCR’s investigation indicated that the company did not (1) adequately implement policies and procedures for authorizing access to the on-line application database; (2) perform an appropriate technical evaluation in response to a software upgrade to its information systems; and (3) have technical safeguards in place to verify the person or entity seeking access to electronic PHI maintained in its application database. As a result, the company impermissibly disclosed the ePHI of 612,402 individuals by allowing access to the ePHI of such individuals maintained in the application database. This data included names, dates of birth, addresses, Social Security numbers, telephone numbers and health information. The case sends an important message to HIPAA-covered entities to take caution when implementing changes to their information systems, especially when those changes involve updates to Web-based applications or portals that are used to provide access to consumers’ health data using the Internet.