Regulatory Update with a Touch of HIPAA

Cloud Communications Alliance Quarterly Meeting
Miami, January 2015

Glenn S. Richards, Partner
Pillsbury Winthrop Shaw Pittman LLP
Phone: 202.663.8215
glenn.richards@pillsburylaw.com

Pillsbury Overview

- With more than 650 attorneys, Pillsbury is a full-service firm with market-leading strengths in the communications, technology, intellectual property, corporate, energy, financial services and real estate sectors.
- Our attorneys are strategically located in 18 offices to serve clients in and outside the United States.
- The Pillsbury communications practice started in 1934 and today represents service providers and investors in all sectors of the industry, including broadcasting, satellite , wireline, wireless and Internet communications.

A Year of Issues that Matter – The A List

- Net neutrality and classification of VoIP
- USF contribution methodology
- VoIP access charges
- IP interconnection
- Access to fiber facilities
- Maintenance of legacy copper networks

A Year of Issues that Matter – The B List

- VoIP provider access to telephone numbers
- Expansion of 911 obligations; NG 911
- Rural call completion reporting obligations
- CALEA update
- Communications Act rewrite
- State PUC, legislative initiatives re: VoIP

A Touch of HIPAA

- The Health Information Portability and Accountability Act of 1996 ("HIPAA") is a federal law that (1) sets national standards for the security of electronic protected health information, and (2) protects the privacy of individually identifiable health information.
- The relevant parts of the HIPAA Rules include the following:
  - The Privacy Rule, which addresses permitted and prohibited uses and disclosures of PHI;
  - The Security Rule, which addresses the administrative, physical, and technical safeguards that are required to ensure the confidentiality, integrity, and availability of electronic PHI; and
  - The Breach Notification Rule, which requires reporting of breaches of unsecured (unencrypted) PHI to affected parties.

A Touch of HIPAA

- HIPAA only applies to “covered entities” and, where provided by statute, to “business associates” of covered entities.
- A “covered entity” under HIPAA is either (1) a health plan, (2) a healthcare clearinghouse, or (3) a health care provider (e.g., hospital, physician, laboratory, etc.) who transmits any health information in electronic form in connection with a transaction (i.e, submits claims electronically).

A Touch of HIPAA

- A “business associate” is an entity that creates, receives, maintains or transmits “protected health information” on a covered entity’s behalf.
- “Protected Health Information” or “PHI” is any information created or received by a health care provider, health plan, employer or health care clearinghouse relating to an individual’s past, present or future health care or payment for health care and that identifies the individual or could be used to identify the individual. Includes medical records, lab reports, email or voice mail left by or sent to a patient.
- Electronic PHI is data which is transmitted or maintained on electronic media. Electronic media is defined as either:
  - Electronic storage material (e.g., computer hard drives), or
  - transmission media (e.g.,the internet.)

A Touch of HIPAA

- Thus, “certain transmissions, including of paper, via facsimile, and of voice, via the telephone, are not considered to be transmissions via electronic media, *if* the information being exchanged *did not exist in electronic form immediately before the transmission*”.
- A common misconception is that HIPAA applies only within the healthcare industry. However, business phone systems that leverage VoIP technology may also fall under the HIPAA regulations.
- Under the Health Information Technology for Economic and Clinical Health Act (HITECH Act) business associates became directly liable under HIPAA, meaning that regulatory oversight and enforcement actions could be taken by federal agencies (including HHS) directly against business associates of covered entities.

A Touch of HIPAA

- The HITECH Act clarified that "data transmission organizations" were required to be treated as business associates when they access PHI on a routine basis. Conversely, data transmission organizations that do not require access to PHI on a routine basis (i.e., entities that act as mere conduits for the transport of PHI but do not access the information) would not be treated as business associates (the "conduit exception"). The conduit exception is a narrow one and is intended to exclude only those entities providing mere courier services, such as the Postal Service, UPS or their electronic equivalents, such as internet service providers (ISPs) providing mere data transmission services. According to HHS, a conduit transports information but does not access it other than on a random or infrequent basis as necessary to perform the transportation service or as required by other law."

A Touch of HIPAA

- A VoIP provider that maintains PHI for a covered entity is a business associate. Temporary storage of transmitted data can meet the conduit exception but storage of PHI (such as emails or recorded voicemails) is considered to be the maintenance of PHI and not eligible for the conduit exception, even if the entity does not actually view the PHI. The business associate determination (and "conduit exception") apply to subcontractors of business associates as well.
- Business associates must implement the safeguards set forth in HIPAA and may be subject to the breach notification requirements in the event of unauthorized access or disclosure of unsecured PHI. PHI can be rendered unusable, unreadable, or indecipherable to unauthorized individuals— "secured" and thus, exempt from the breach notification obligations, only through encryption or destruction.

A Touch of HIPAA

- What does the Security Rule require? A partial list:
-
  - Ensure the confidentiality, integrity, and availability of electronic PHI;
  - Protect against reasonably anticipated threats or hazards to the security or integrity of PHI;
  - Ensure compliance by workforce;
  - Comply with the more than 20 security standards described in the Rule; and
  - Maintain, review, and modify security measures as needed.

A Touch of HIPAA

- What does the Privacy Rule require? A partial list:
-
  - Using or disclosing only the minimum amount of PHI necessary to accomplish the purpose of the use or disclosure;
  - Entering into business associate contracts with any subcontractors that are business associates;
  - Using and disclosing PHI only for purposes permitted by the Rule;
  - Not engaging in certain uses or disclosures without the individuals' authorization;
  - Maintaining a record of disclosures of PHI and providing an accounting of those disclosures upon request, etc.;
  - Maintaining written privacy policies and procedures, and updating those policies from time to time; and
  - Training workforce members on privacy policies and procedures.

A Touch of HIPAA

- What does the Data Breach Notification Rule require?
-
  - Report breaches of unsecured PHI (essentially, PHI that is not encrypted in accordance with standards adopted by HHS) to the covered entity;
  - Covered entities in turn are required to report those breaches to HHS and, in some cases, the news media; and
  - Parallel state laws often require reporting to local law enforcement and/or consumer privacy protection agencies.

A Touch of HIPAA

- Business associates must enter into business associate contracts.
- Covered entities and business associates are required to enter into a business associate contract with each business associate or subcontractor that creates, receives, maintains, or transmits PHI on their behalf.
- Business associate contracts will summarize the rules described above, and usually add additional obligations with respect to the privacy and security of PHI.

Q&A