Getting on the Omni “Bus”

Route Planning

- Identify road blocks and bypass construction delays
- Obtain travel insurance and avoid moving violations
- Use safety equipment
- Inform all passengers the rules of the road
- Arrive timely
Road Map

Health Insurance Portability and Accountability (HIPAA) Act of 1996

Health Information Technology for Economic and Clinical Health (HITECH) Act

Omnibus Final Rule

The Omnibus Travel Schedule

- The Final Rule was published January 25, 2013
- The Final Rule became effective on March 26, 2013
- The compliance date was six months from the effective date: September 23, 2013
- HHS provides an extended compliance deadline of one additional year to enter into BAAs that comply with the Final Rule but only if the BAA in question was in existence prior to the issuance of the Final Rule on January 25, 2013.
Safety Equipment

Update and Revise:
- Policies and Procedures
- Notice of Privacy Practices (NPPs)
- Data Breach Risk Assessment Tools
- Business Associate Agreements (BAAs)
- Restrictions on the sale of Protected Health Information (PHI)
- Marketing and fundraising restrictions
- Training/Education on proper use of equipment

Passengers

- Covered Entities (CEs)
- Business Associates (BAs)
- Business Associate Agreements
- Contract Revisions
- Training and Education
- Sub-Contractors
- Workforce
Bus Stops

1. NPPs
2. BAs and BAAs
3. Data Breach Assessment
4. Right to request a restriction
5. Individual’s Right of Access
6. Marketing
   - Sale of PHI
   - PHI and Fundraising
7. School Immunizations
8. PHI of Decedents

Bus Stop #1: Notice of Privacy Practices (“NPP”)

- The Final Rule required several changes to our current NPP. Those changes will be most generally related to the use and disclosure of psychotherapy notes, for marketing purposes, and the sale of PHI.
- Evaluate and make the necessary changes to all Notices of Privacy Practice including those where state specific requirements may exist, i.e., Pennsylvania and Texas.
- Oversee the distribution the NPP accordingly to include:
  - Time of patient registration
    - Facility web site (hospitals, physician practices, etc.)
    - Posters
Notice of Privacy Practices ("NPP") Next Steps

Responsibilities will include:

• Conducting an inventory of all service areas where the NPP is to be posted. Be sure to include all service lines (e.g., Physician Practices, ASCs, Rehabilitation Centers, etc.)

• Conduct walk-through reviews to remove all out-dated versions of the NPP

• Follow through to assure NPP Posters are posted

Business Associate

• The Final Rule significantly modifies the definition of a business associate

  “Prior; limited to entities that “use or disclose” PHI in order to provide a service on behalf of a covered entity

  Now; includes any organization that “creates, receives, maintains, or transmits PHI for a function regulated by HIPAA”

• The Final Rule excludes ‘conduits’ of PHI such as UPS and USPS. This is a narrowing of the ‘conduit’ exception.
Business Associate

- Entities that, under the expanded definition, are considered business associates:
  - ✔ Patient Safety Organizations
  - ✔ Health Information Organizations (HIO)
  - ✔ E-Prescribing Gateways
  - ✔ Vendors of Personal Health Records

- Persons or entities that provide data transmission services with respect to PHI and that requires routine access to PHI

- Fact specific based upon the nature of the service and the extent to which the entity needs access to PHI to perform the service for the covered entity.

Business Associate

- Conduit exception is narrow and is intended to exclude only those entities providing mere courier service (USPS, UPS, and ISPs).

- An entity that maintains PHI on behalf of a covered entity is a business associate and not a conduit, even if the entity does not view the PHI.

- Data storage company that has access to PHI (electronic or hardcopy) is a business associate even if the entity does not view the information or does so on a random or infrequent basis.

- Cloud (“SaaS”) and Application Service Providers (“ASP”)
Business Associate

• What have we done?
  ✓ We have updated the current BAA to incorporate the changes brought about by the Omnibus Rule.
  ✓ We are reviewing the active contracts in our contract management system to identify those relationships that are or may be business associates.
  ✓ We have made modifications in our contract management system to track business associates.
  ✓ We developed a detailed plan used to walk the Facility Privacy Officers through what will undoubtedly be a major process.

Business Associate

• What have we done?
  ✓ We have provided education to contract administrators and FPOs about the ‘business associate.’
  ✓ We have engaged the FPO to review the inventory of active contracts at the FPO’s facility(ies) and determine whether they are or are not a business associate.
  ✓ Communicated and distributed the revised BAA to the existing business associates

• What are we doing now?
  ✓ Reviewing requests from BAs to re-negotiate the terms of our BAA
  ✓ Continue the revised processes going forward to properly identify BAs and have required BAAs in place.
Business Associate Addendums

Technical changes in Omnibus where OCR includes commentary that entities define in their business associate agreements the requirements of how, when and to whom a data breach should be reported.

Data Breach Notification

“The provision of the omnibus regulation that has generated the most discussion so far – and that will have the most substantial impact of the overall health care community – is the elimination of the “risk of harm” standard for breach notification.”

The breach notification regulations that covered entities have been following for the last two years have not changed under the Final Rule. The change is the breach notification trigger.
Data Breach Notification

The Final Rule modified the definition of a “breach” as:

An impermissible use or disclosure of PHI is presumed to be a breach unless the covered entity or business associate...demonstrates that there is a low probability that the PHI has been compromised.

Breach notification is necessary in all situations except those in which the covered entity demonstrates that there is a low probability that the PHI has been compromised (or one of the other exceptions to the definition of breach applies).

Data Breach Notification

The Final Rule removed the harm standard and modified the risk assessment to focus more objectively on the risk that the PHI has been compromised.

“If PHI is encrypted pursuant to prior guidance, then no breach notification is required.
Failure to comply with the minimum necessary provision may implicate the obligation for a risk assessment and possibly a data breach notification.
The ‘treated as discovered’ provision is unchanged and underscores the importance of continued workforce training.”
Bus Stop #4: **Right to Request a Restriction**

The Right was introduced as part of HITECH and permits an individual to restrict the disclosure of PHI to a Health Plan when the individual pays in full and out of pocket. There were several modifications made under the Final Rule. Compliance with the patient’s request continues to be required. However:

- The Final Rule does not require a separate Medical Record for the service.
- Medicare and Medicaid audits, as required by law, allow disclosure of ‘restricted’ PHI as such disclosure are exempt from this provision.
- If a state or other law requires the submission of a claim to a health plan for a covered service AND provides no exception to the requirement, the disclosure of PHI is considered legally mandated and is exempt from this restriction.
- Medicare does contain an exception to the provision which allows an individual to refuse submission of a claim for a service. In such cases, the health care provider may accept the out of pocket payment and restrict the disclosure.
- The Secretary provided extensive additional commentary on the many operational issues surrounding this provision.

---

Bus Stop #5: **Individual’s Right of Access**

The Omnibus Rule significantly strengthens the rights of the individual to access the individual’s PHI maintained electronically in one or more designated record sets irrespective of whether the designated record set is an electronic health record (“EHR”).

Those include:

- The form and format of the PHI provided in response to such request (may include .pdf, Word, and Excel)
- The electronic links to images and other data, the images or the other data that is linked must also be included in the electronic copy
Individual’s Right of Access

- Covered entities are not required to scan paper documents to provide electronic copies.
- Covered entities are not required to accept external media devices from individuals if the facility’s risk analysis has determined there is an unacceptable level of risk.
- Covered entities may not then require individuals to purchase a portable device from the covered entity.
- The individual may opt for an alternative form to receive the electronic copy such as email.
- Covered entities are required to transmit the copy of the PHI directly to another person designated by the individual.
- The request must be in writing.
- The request must be signed by the individual.
- The request must clearly identify the designated person.
- The request must clearly state where to send the PHI.

- The use of unencrypted email to provide an electronic copy of the record is permitted under the Final Rule:
  - If the covered entity has advised the individual of the risk AND the individual still prefers the unencrypted email.
  - A ‘duty to warn’ provision must be implemented but does not need to educate individuals about encryption technology and information security.
- The covered entity is not responsible for unauthorized access of PHI while in transit to the individual based upon the individual’s request.
- The covered entity is not responsible for safeguarding information once delivered to the individual.
**Bus Stop #6:**

**Marketing**

- The Final Rule revises and expands the definition of ‘Marketing.’ Those disclosures that are considered ‘marketing’ under the revised definition will require an individual’s authorization.
- The definition now includes communications about health-related products or services if the covered entity receives ‘financial remuneration’ in exchange for making the communication from the products sponsor.
- “Financial Remuneration” is defined to include payments in exchange for making a marketing communication. It does not include non-financial benefits.

---

**School Immunizations**

- Under the Final Rule, a covered entity may provide the immunization records of a student to a school upon the assent of the parent, guardian, or person acting *in loco parentis*.
- The agreement is effective until revoked
- The facility must document, in a manner determined by the facility, the agreement
- The request cannot come from the school
- The covered entity is permitted to release information to state immunization registries where required to do so by law

---

1. *To act in the place or role of a parent.* Its generally accepted common law meaning refers to a person who has put himself/herself in the situation of a lawful parent by assuming the obligations incident to the parental relation without going through the formalities necessary to legal adoption. [Barron's Law Dictionary]
PHI of Decedents
The Final Rule expands the scope of who a covered entity can release the PHI of a decedent to:
Family members or others who were involved in the care of the patient
Those involved in the payment for care prior to the death of the patient
Unless this is inconsistent with the prior expressed wishes of the decedent

Travel Insurance
Meet deadlines established for compliance with the Rule by performing:
✓ training/education
✓ process updates
✓ vendor evaluation
✓ contract management
Moving Violations

The Final Rule retained the categories of violations and respective penalty amounts available.

<table>
<thead>
<tr>
<th>Violation Category</th>
<th>Each violation</th>
<th>All such violations of an identical provision in a calendar year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Did Not Know</td>
<td>$100-$50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Reasonable Cause</td>
<td>$1,000-$50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Willful Neglect – Corrected</td>
<td>$10,000-$50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Willful Neglect – Not Corrected</td>
<td>$50,000</td>
<td>$1,500,000</td>
</tr>
</tbody>
</table>

Moving Violations

- Determination of Civil Monetary Penalty (“CMP”)
- The CMP imposed will be based upon case-by-case basis
- Change in terminology in the Final Rule
  - From: “history of violations”
  - To: “previous indications of non-compliance”
  - Implication: allow consideration of prior non-compliance even when there was no formal finding of a violation
- Investigations
  - OCR must initiate an investigation if preliminary review indicates a possible violation due to willful neglect; no longer discretionary.
  - OCR has discretion to resolve violations formally or informally; no longer obligated to seek informal resolution.
Accounting of Disclosures ("AoD")

The modifications to the Accounting of Disclosure provision were not included in the Omnibus Rule. The release of AoD Final Rule is unknown.

Finally, the Good News

The Omnibus Final Rule has modified the definition of Protected Health Information to provide that the Privacy and Security Rule do not protect the individually identifiable health information of persons who have been deceased for more than 50 years.

The End!
Deals/Packages

A few value-added benefits

- Contract Management processes (e.g., creation/renewal of agreements not otherwise in place
- BA identification processes
- Updated tools including data breach risk analysis, policies and procedures, and revised BAAs
- Training/education efforts for all involved parties

Questions?