Margaret Hambleton
Vice President, Corporate Compliance Officer
Dignity Health

"Section 1179 of the Health Insurance Portability and Accountability Act"
Subcommittee on Privacy, Confidentiality & Security
National Committee on Vital and Health Statistics
May 6, 2015
National Center for Health Statistics
Hyattsville, MD

Introduction

- Good afternoon and thank you for the opportunity to participate in this timely discussion.
- My name is Margaret Hambleton. I am the Vice President and Corporate Compliance Officer for Dignity Health.
- Dignity Health is one of the nation's five largest health care systems with 38 hospitals in 3 states and more than 350 care sites throughout the United States.
- As we know, the delivery of health care is transforming in dramatic ways to achieve better patient access, better care to individual patients and populations of patients, and a more efficient and cost effective health care delivery system.
- This transformation requires health care providers like Dignity Health to develop new partnerships and to engage with our existing partners in new and innovative ways.
- Given the complexity in the delivery of health care, Covered Entities such as Dignity Health must rely on numerous third parties to help us fulfill our responsibilities to our patients. Often, this requires sharing health care information with these third parties.
- More and more often, we are looking to our traditional banking partners to provide some of these needed services. We have historically considered these partners exempt from HIPAA

under section 1179. However, with the new and expanding services offered by financial institutions, compliance professionals for Covered Entities need to look more carefully at whether the exception continues to apply.

- Typically, these expanded services include the provision of lock box services and participation in due diligence efforts, particularly with bond or equity offerings.
- In the future, the role of financial institutions could be significantly further expanded. This makes it necessary for Covered Entities and their compliance efforts to:

  1) ensure services provided by financial institutions are analyzed to determine the extent to which they will need to be considered Business Associates;

  2) ensure appropriate Business Associate Agreements are in place; and,

  3) determine the extent to which these institutions comply with their obligations as Business Associates.
- At Dignity Health, we have devoted significant resources in staff and technology to comply with HIPAA and the Final Omnibus HIPAA Rules. Even so, ensuring our compliance efforts with the three points above can be challenging.

Determining When a Financial Institution is a Business Associate

- The Final Rule expands the definition of Business Associate to generally include a person that creates, receives, maintains or transmits Personal Health Information (or PHI) on behalf of a Covered Entity (rather than for its own purposes). Generally speaking, financial institutions that use or disclose PHI to perform services for a Covered Entity should be considered a Business Associate.

- Health care compliance professionals are often challenged, not in determining when a financial institution is a Business Associate, but when the *relationship* changes from a traditional financial partnership covered under section 1179, to a non-traditional partnership requiring a Business Associate Agreement.
- Part of the challenge is due to the variety of origination points of such relationships (through Treasury, Finance, Patient Accounting, and others) and also a lack of understanding about agreement requirements when the relationship changes.
- It is critical for our workforce to engage with our financial partners for both parties to understand the difference in the relationship and recognize when such services require a Business Associate Agreement.

Ensuring Appropriate Business Associate Agreements are in Place

- Once the determination is made that the services provided by a financial institution require a Business Associate Agreement, it important that the Covered Entity evaluate the extent to which the Business Associate has the capacity for compliance with HIPAA and ensure an appropriate Business Associate Agreement is in place.
- Business Associates, including financial institutions that are business associates, are statutorily obliged to comply with certain HIPAA provisions, including conducting a security rule risk assessment, developing policies and procedures, conducting workforce training, and establishing administrative, physician, and technical safeguards.
- Covered Entities must evaluate through some prospective analysis that the Business Associate can adequately comply.

- Given resource constraints, this can often be challenging. It becomes more challenging with financial institutions that have generally not developed mature HIPAA compliance programs.
- A critical key to a successful partnership requires the Covered Entity to develop robust due diligence tools to evaluate risk and financial institutions. At Dignity Health we have developed a Security Risk Assessment tool to evaluate compliance with the HIPAA Security Rule and a Privacy Impact Assessment to determine risks related to compliance with the components of the Privacy Rule our Business Associates are responsible for. Our Financial Institutions are also required to ensure they have developed the internal structures necessary to ensure compliance.
- Even so, keeping an accurate inventory of Business Associates is a challenge for Covered Entities such as Dignity Health due, in part, to the sheer volume of agreements we have in place.
- This is made more complicated because of the many points of origin for Business Associate relationships across the enterprise.

Ensuring On-Going Compliance

- While HITECH made Business Associates strictly accountable to regulators for failure to comply with the HIPAA Security Rule and some provisions of the HIPAA Privacy rule, Covered Entities have some oversight responsibility for their Business Associates.
- This oversight and compliance monitoring function tend to audit “high risk” functions and services and often focuses on periodic security risk assessments and privacy impact assessments.

Recommendations for Improving Compliance

- To improve overall compliance, Dignity Health believes education and training are key for both Covered Entities and Business Associates.

- In addition, we are supportive of a process for voluntary Third Party Certification which would enable our Business Associates to provide us with certain assurance that they meet a minimum level of compliance and allow Covered Entities to free up certain resources required to manage Business Associates.
- Dignity Health would welcome standardization related to Business Associate Agreements, due diligence reviews, security and privacy assessments, monitoring tools, and independent audits or certifications that could further reduce the burden of HIPAA compliance
- Meetings like this are an important step to helping the community and policy makers increase awareness and understand the expanding role of our financial institutions play in health care delivery. Dignity Health appreciates the opportunity to participate and looks forward to any additional outreach, education, assistance and guidance that may come from this important discussion.