HIPAA's Impact on Depository Financial Institutions

2nd National Medical Banking Institute

Rick Morrison, CEO
Remettra, Inc.
rick.morrison@remettra.com

Remettra

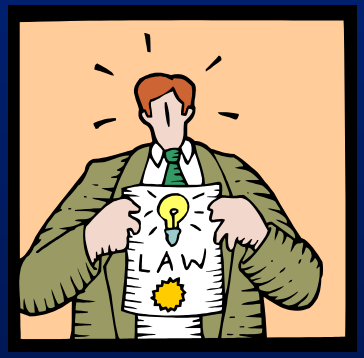
HIPAA

Disclaimer…

- Don’t have all the answers
- Don’t even know all the questions
- Comments consistent with legal advice

What is HIPAA?

- Health Insurance Portability and Accountability Act of 1996
- One purpose of HIPAA is to improve the efficiency and effectiveness of the health care system.
- The stated intent of HIPAA's privacy regulation is to address public concerns by regulating entities that possess PHI.



Remettra

Compliance Dates

- HIPAA Standards for the Privacy of Individually Identifiable Health Information: ***April 14, 2003***
- HIPAA Standards for Transaction Code Sets: October 16, 2002 (2003 if a covered entity files for an extension)
- HIPAA Standards for Security: April 21, 2005

Why Privacy Regulation

HIPAA's privacy regulation is an attempt to address a growing public concern that advances in electronic technology and the resulting evolution in the health care industry may result in a substantial loss of the privacy surrounding patient health information.

Public Perception

- 84% of those surveyed in 1999 agreed with the statement that they had "lost all control over their personal information." The Standards for Privacy of Individually Identifiable Health Information; Final Rule; 45 CFR Parts 160 and 164; p.82465
- Another survey found that 35% of Fortune 500 companies look at people's medical records before making hiring and promotion decisions. Starr, Paul. "Health and the Right to Privacy," American Journal of Law and Medicine, 1999. Vol. 25, pp. 193-201
- A national survey conducted in January, 1999 found that one in five Americans believe their health information is being used inappropriately. California HealthCare Foundation, "National Survey: Confidentiality of Medical Records" January, 1999 (http://www.chcf.org)

Gramm-Leach-Bliley

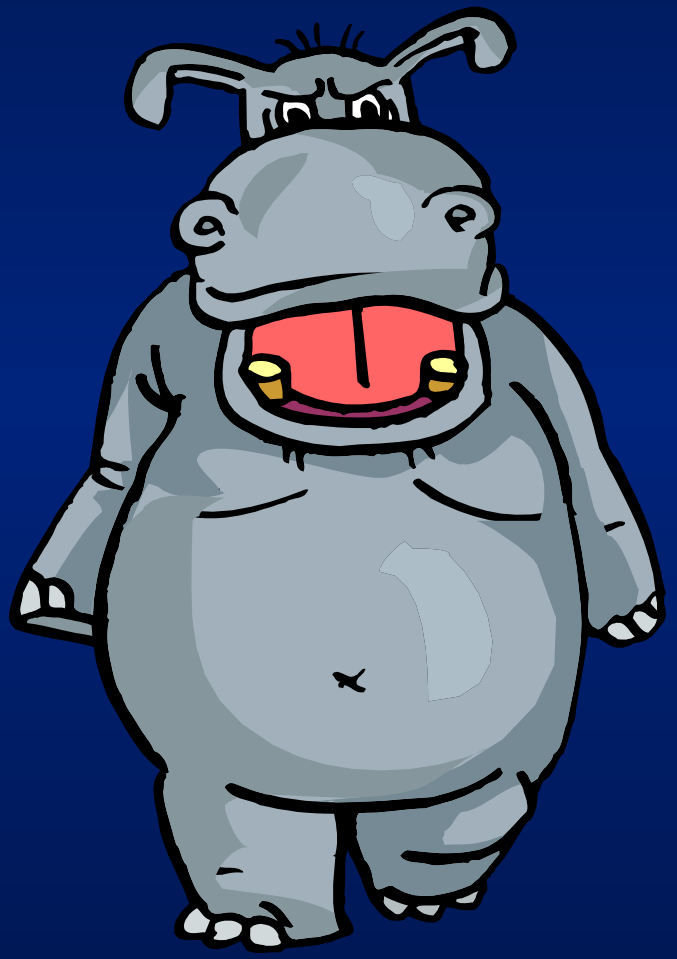
- The Gramm-Leach-Bliley Act (GLB) protects consumers from financial institutions sharing information with third parties, but it does **NOT** protect consumers from financial institutions using PHI in its own operations as a risk assessment tool (loan approval, etc).
- GLB allowed banks to continue their business as usual unless the customer took action to opt out.
  - ***HIPAA does not provide this allowance*.**

DHHS

- The Department of Health and Human Services (DHHS) was authorized by Congress to author, ***interpret*** and disseminate HIPAA's administrative regulations.
- Published preamble of the HIPAA Privacy Regulation and DHHS comments specifically address banking functions and HIPAA's impact on those functions.
- The Final Security Rule does not specifically mention financial institutions.

What Has DHHS Said?

Review of published comments concerning HIPAA's impact on banking



Section 1179

"To the extent that an entity is engaged in activities of a financial institution or is engaged in authorizing, processing, clearing, settling, billing, transferring, reconciling, or collecting ***payments***, for a financial institution, this part and any standard adopted under this part, shall not apply to the entity with respect to such activities, …"

- The key word in Section 1179 is "**payments**"
- Section 1179 does not address "**remittance advices**"

Privacy Rule: pp. 82615-82616

- "Since the EFT is used to initiate the transfer of funds between the accounts of two organizations, typically a payor and a provider, it includes no individually identifiable health information not even the names of the patients whose claims are being paid…"
- "The ERA, on the other hand, contains specific information about the patients and the medical procedures for which the money is being paid and is used to update the accounts receivable system of the provider."
- "This information [ERA] is always needed to complete a standard Health Care Payment and Remittance Advice transaction, but is never needed for the funds transfer activity of the financial institution."

Privacy Rule - Section 164.501

- "…information to effect funds transfer is transmitted in a part of the transaction separable from the part containing any individually identifiable health information."

- "We note that ***a covered entity may conduct the electronic funds transfer*** portion of the two payment standard transactions [Health Care Payment and Remittance Advice (835) and Health Plan Premium Payments (820)] with a financial institution without restriction, ***because it contains no protected health information***."

- "The protected health information contained in the electronic remittance advice or the premium payment enrollee data portions of the transaction is not necessary either to conduct the funds transfer or to forward the transaction."

Privacy Rule - Section 164.501

- "Therefore, ***a covered entity may not disclose the protected health information to a financial institution for these purposes [electronic funds transfer]***."

- "A covered entity may transmit the portions of the transactions containing protected health information through a financial institution ***if the protected health information is encrypted*** so it can be read only by the intended recipient [Healthcare Providers (835) or Health Plans (820)]."

- "In such cases, ***no protected health information is disclosed and the financial institution is acting solely as a conduit*** for the individually identifiable data."

Privacy Rule: p. 82616

- "Under the **proposed** Security Rule, the ACH system and similar systems would have been considered ***"open networks"*** because transmissions flow unpredictably through and become available to member institutions who are not party to any business associate agreements (in a way ***similar to the internet***)."
- ***"The proposed Security Rule would require any PHI transferred through the ACH or similar system to be encrypted."***

Final Security Rule

The Final Security Rule removed any reference to financial institutions or the ACH system.

Covered entities must establish procedures to ensure the protection, confidentiality, integrity, and availability of healthcare information.

Final Security Rule

- To comply, the final rule requires the establishment of administrative, physical, and technical safeguards.
- One of the technical safeguards is transmission security.
- Covered entities must implement techniques, such as encryption, to protect health information during electronic communication.

Final Security Rule

In the Final Security Rule, “integrity controls” and “encryption” are “addressable implementation specifications”.

Protection must be commensurate with the associated risk.

HIPAA's Impact on Health Plans

- HIPAA mandated regulations require health plans to provide electronic remittance advices to providers upon request.
- As a result, health plans will lose the efficiencies of a single system and will incur higher operating expense, lower productivity, and more demanding customer service under dual paper and electronic systems.
- This can negate savings during the transition to an electronic environment.

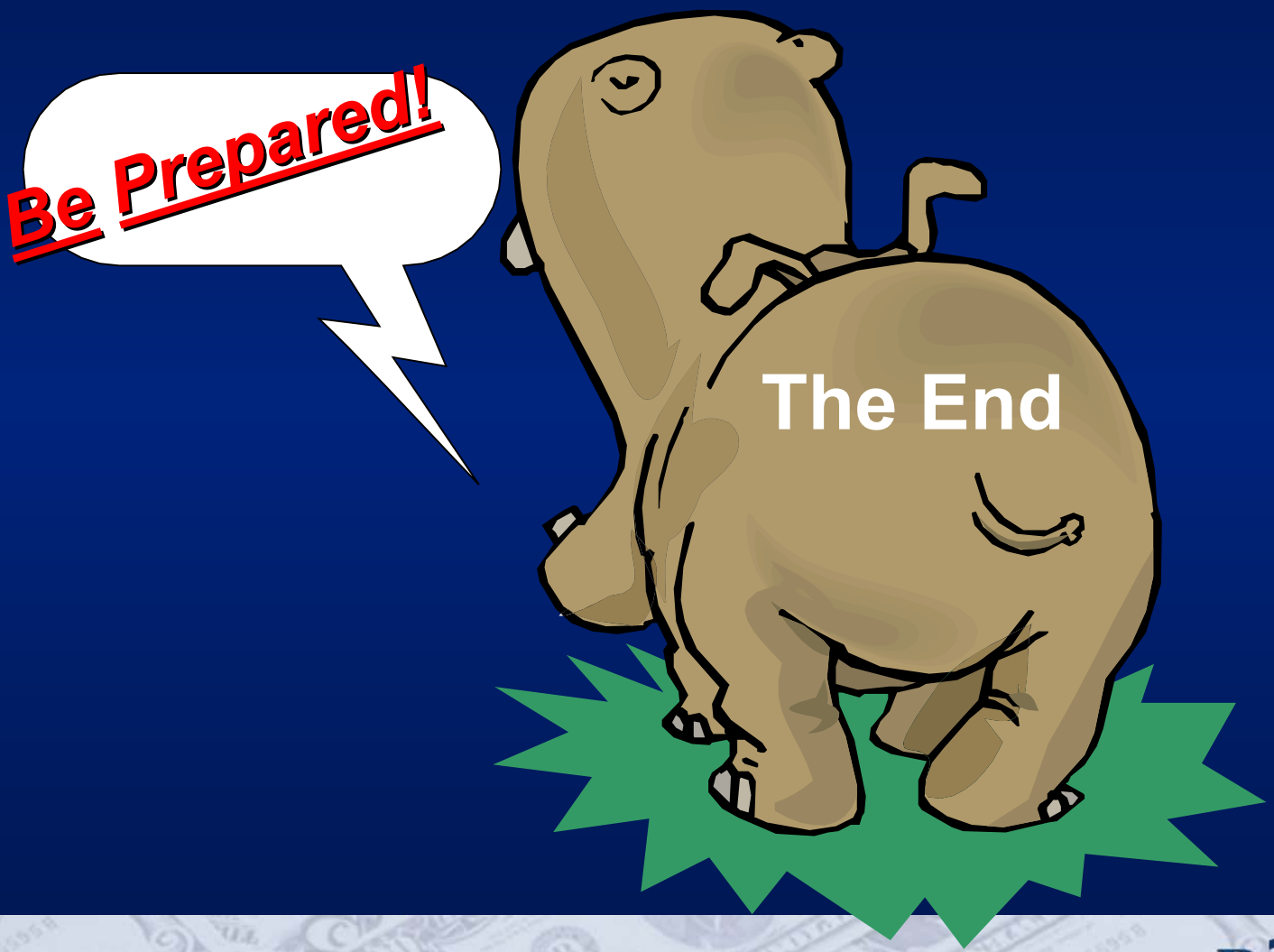
Hurdles for Banks

Examples:

- Can the ODFI guarantee the Provider's bank is capable of transmitting the 835 to the Provider?
- Will all RDFIs be willing to sign Business Associate Agreements with Providers?
- Can a Payor require a Provider to change banks in order to receive the 835?
- Business Associate Agreements:

  ODFI → ACH Operator → RDFIs

Don't Forfeit the Opportunities Provided By HIPAA



Remettra