# *HIPAA*
# *&*
# *The ACH Network*

**The Medical Banking Institute**

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

# HIPAA

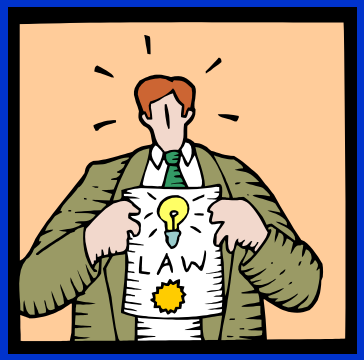
## Disclaimer…

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

Remettra

# 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

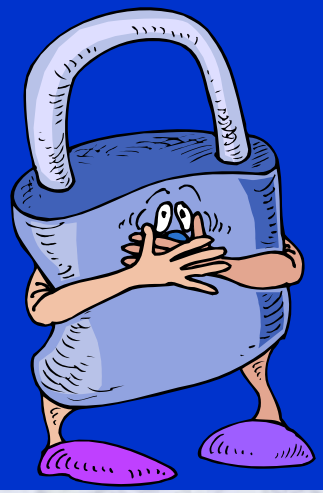
# Compliance Dates

- 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:  To Be Determined

Remettra

# 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.



Remettra

# 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)

Remettra

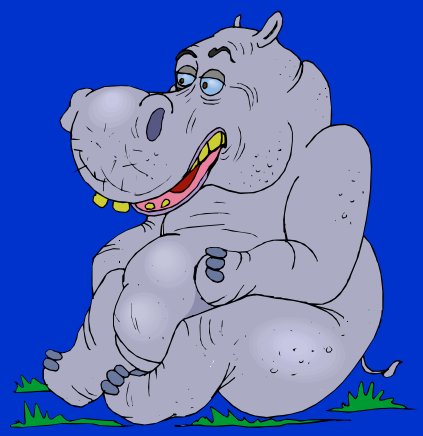
# Gramm-Leach-Bliley

The Gramm-Leach-Bliley Act 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).

Remettra

# HIPAA & Financial Institutions

- Although some financial institutions may have “privacy policies”, there is no applicable law or regulation regarding the use of PHI within a financial institution outside of HIPAA.
- Therefore, without HIPAA’s regulations, it would be purely at the financial institution’s discretion as to if, or how, that information would be used.



Remettra

# Nightmare Scenario

**Consider this scenario:**

- Customer requests a loan
- Bad credit history – deny the loan request
- Customer's health plan discloses PHI to the bank
- Customer happens to be HIV positive
- Customer files a lawsuit
- Financial Institution had "*opportunity*" and "*motive*"
- Now, the issue is proof
  - Has the bank ever approved a loan request for a customer with equal or worse credit history?
  - Can the bank prove that it had sufficient safeguards in place to preclude access by the loan officer to the customer's PHI?
  - Would a jury believe the financial institution without adequate documentation and proof?

Remettra

# HIPAA & Financial Institutions

**Does the preceding sound absurd?**

- If so, consider the fact that a banker on a state health commission accessed a list of local cancer patients, cross-referenced it to a list of bank customers who had outstanding loans, and used the medical information to call in the loans of the cancer patients. M. Lavelle, "Health Plan Debate Turning to Privacy: Some Call For Safeguards on Medical Disclosure. Is a Federal Law Necessary?" The National Law Journal, May 30, 1994, p. A1

- Under the penalty provisions of HIPAA, this privacy violation for a **covered entity** is an illegal activity and could trigger a 10-year imprisonment and as much as $250,000 in penalties.

Remettra

# HIPAA & Financial Institutions

- Financial institutions that receive patient information easily could find themselves operating under a shadow of suspicion as the public becomes aware that their financial institution may be receiving their PHI.

- As the public, and their attorneys, become aware that their financial institution may be receiving their PHI, the potential for ***alleging*** a violation of patient privacy and the risk of litigation escalates, producing a scenario that can be devastating to a financial institution's reputation.

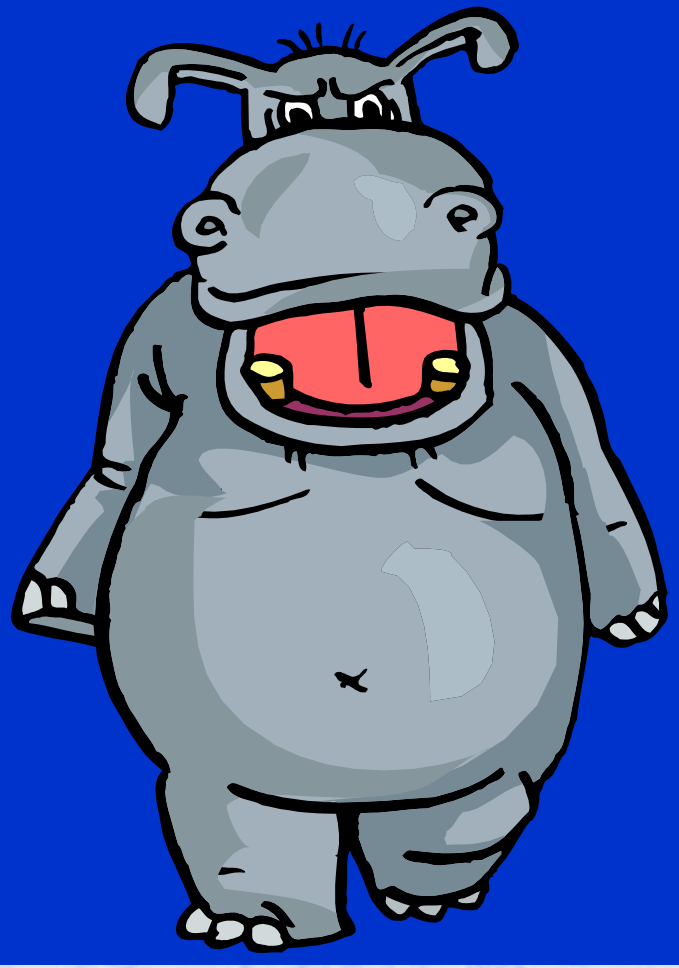
Remettra

# DHHS

- The Department of Health and Human Services (DHHS) was authorized by Congress to author, ***interpret*** and disseminate HIPAA's administrative regulations.
- Published preambles to the HIPAA regulations and DHHS comments specifically address banking functions and HIPAA's impact on those functions.

# What Has DHHS Said?

Review of published comments concerning HIPAA's impact on banking



Remettra

# 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**"

Remettra

# 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."

Remettra

# 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."

Remettra

# 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."

Remettra

# 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."***

Remettra

# DHHS's Published Position

- Other private industry legal counsel conclude that DHHS intends that a financial institution may receive the remittance advice containing PHI and forward it through the ACH network as a CTX file to the provider's bank **as long as the remittance advice is encrypted** so that the PHI can not be read by the RDFI.
- However, financial institutions may receive payment information (no PHI) and forward the payment as a CCD+ file to the provider's bank.

Remettra

# Banks as Clearinghouses

- It is widely accepted that the definition of a “healthcare clearinghouse” was written to cover any service company, regardless of their industry, that performs the specific functions DHHS uses to define a clearinghouse.

- Therefore, it seems apparent that DHHS’ definition of a clearinghouse can apply to depository financial institutions.

Remettra

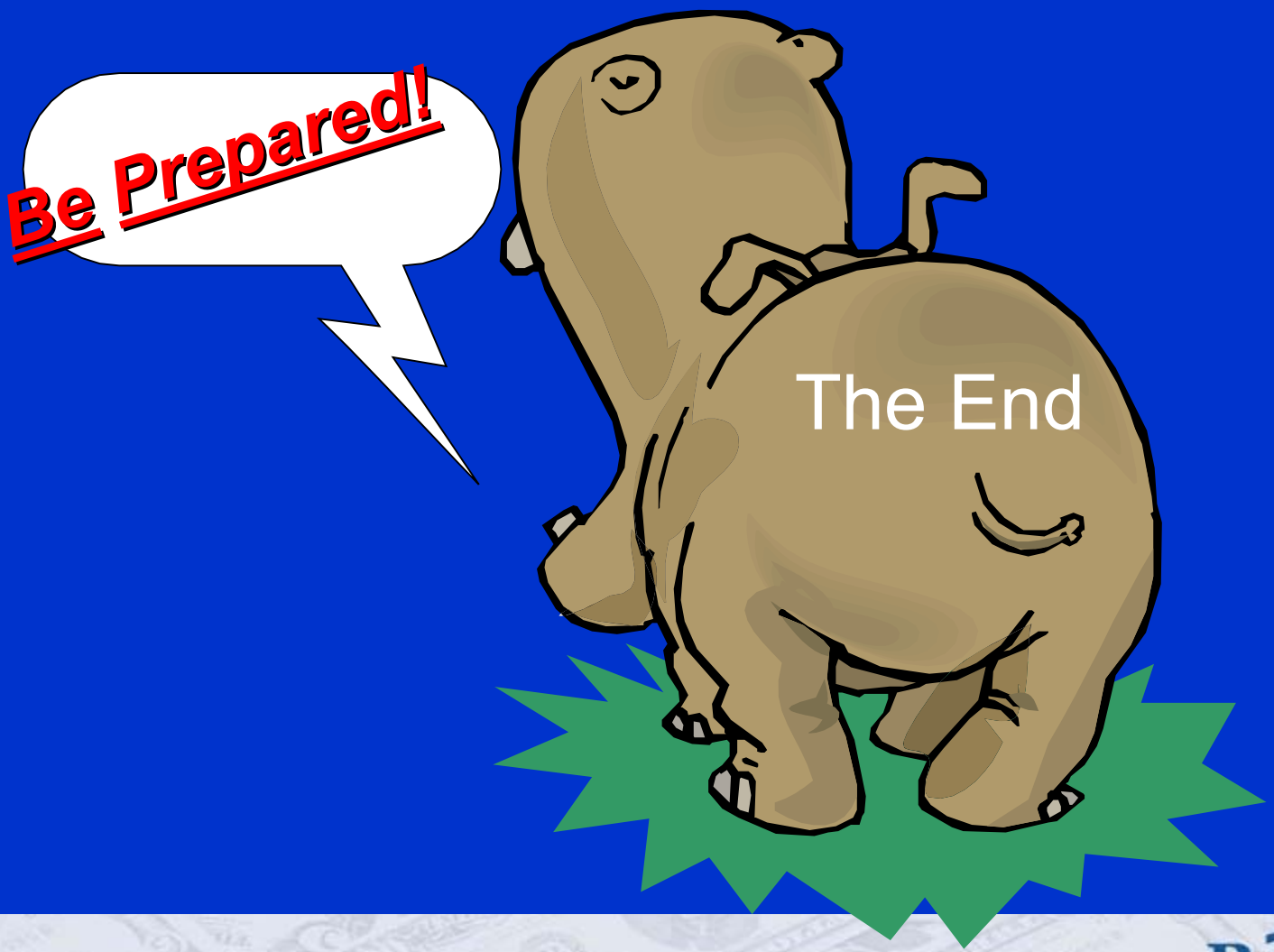
# Banks as Clearinghouses

**HIPAA experts agree that:**

- The determining factor of whether a financial institution is a clearinghouse or a business associate resides in what the financial institution does, not in what a financial institution declares itself to be.
- The determination of whether a financial institution is considered a clearinghouse is ***NOT*** dependent upon the type of service specified in the contract with a customer.
  - ***Law defines contracts; contracts don't define law.***

Remettra

# Don't Forfeit the Opportunities Provided By HIPAA




Remettra