



EHNAC

Electronic Healthcare Network Accreditation Commission

Privacy & Security Issues & Update: New HIPAA/HITECH Financial Compliance Guide and Privacy NPRM Webinar

Panelists

Lee Barrett, EHNAC, Moderator

John Casillas, SVP, HIMSS Medical Banking Project

Alberto Casas, Director, CitiBank

Jan Estep, President & CEO,

NACHA - The Electronic Payments Association

Sharon Klein Esq, Pepper Hamilton LLP

June 15, 2011



EHNAC

Electronic Healthcare Network Accreditation Commission

Agenda for Webinar Today

- White Paper Objective/Key Findings
- Overview of Applicable Regulations (HIPAA & HITECH)
- Banking + Healthcare + ACH = The NACHA Factor
- The March Towards Electronic Business Transformation in HC
- EHNAC & Financial Institution Perspective





EHNAC

Electronic Healthcare Network Accreditation Commission

White Paper Sponsored by:

Electronic Healthcare Network Accreditation Commission

www.ehnac.org

© 2010 Electronic Healthcare Network Accreditation Commission, All Rights Reserved



Healthcare Information and Management Systems

<http://www.himss.org/ASP/index.asp>

© 2010 Healthcare Information and Management Systems Society, All Rights Reserved



NACHA – The Electronic Payments Association

<http://www.nacha.org/>

© 2011 NACHA -- The Electronic Payments Association. All rights reserved.



Workgroup for Electronic Data Interchange

www.wedi.org

© 2010 Workgroup for Electronic Data Interchange, All Rights Reserved



EHNAC

Electronic Healthcare Network Accreditation Commission

White Paper Objectives & Key Findings



- The passage of the Health Information Technology for Economic and Clinical Health Act (HITECH) directly affects those financial institutions that provide specialized services for the healthcare sector.
 - Updated privacy and security rules
 - Expansion of business associate regulations
 - New breach reporting requirements
 - Tougher penalties



EHNAC

Electronic Healthcare Network Accreditation Commission

White Paper Objectives & Key Findings (cont.)

- Financial institutions that serve healthcare customers must determine whether HIPAA and HITECH are applicable to them.
 - Does the organization have access to protected health information (PHI) through the services provided to organizations within the healthcare sector? If so:
 1. Determine if designation is Covered Entity or Business Associate
 2. Implement appropriate healthcare privacy and security program with the required controls framework





HIPAA Covered Entities

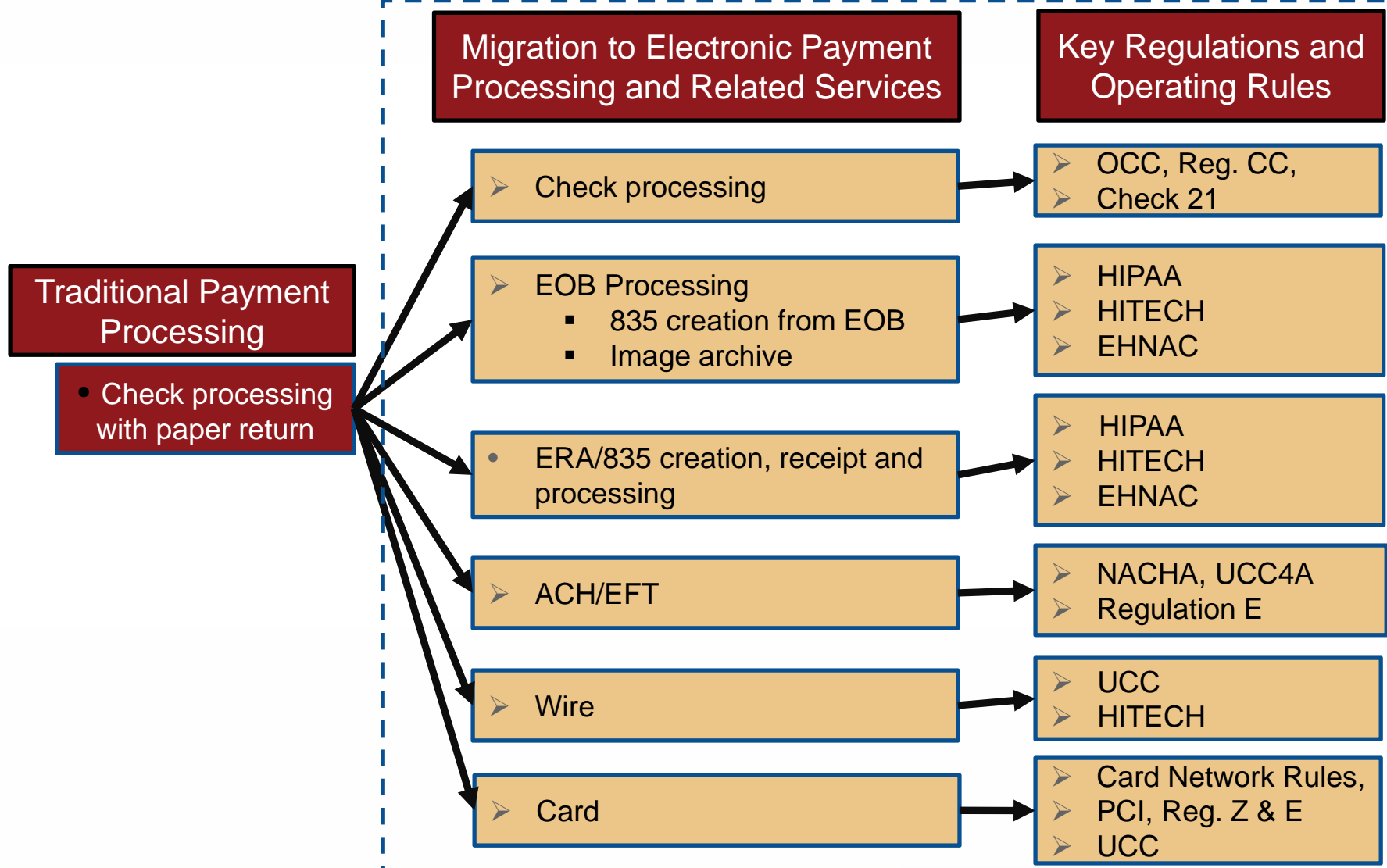
Covered Entity	Examples
Health Plan	Health insurance issuer, an MHO, Medicare, Medicaid
Healthcare Clearinghouse	A billing service, repricing company, community health information system, "value-added" network
Healthcare Provider	Includes facilities such as hospitals and clinics as well as individuals such as doctors, nurses and other medical specialists.



EHNAC

Electronic Healthcare Network Accreditation Commission

Evolution of Financial Services and Resulting Rules and Regulations





EHNAC

Electronic Healthcare Network Accreditation Commission

Establishing the Healthcare Privacy/Security Program Identify Key Players and Responsibilities



- Who is the corporate sponsor with oversight responsibility of the compliance program to ensure the privacy and security of protected health information?
- Who is the designated Privacy Officer or Security Officer?
- Who is responsible for working with the officers to represent each business unit and work to maintain compliance?



Compliance Program Roles and Responsibilities

Role	Possible Responsibilities
Chief Compliance Officer / Corporate Sponsor	<ul style="list-style-type: none">➤ Oversee compliance program; develop & maintain formal HIPAA program.➤ Complete periodic risk assessments of individual business units and communicate results.➤ Provide subject matter expertise in application of HIPAA Privacy and Security Rules.➤ Monitor regulatory changes and work with team to identify impacts and required program changes.➤ Serve as a member of the HIPAA Incident Response Team.



Compliance Program Roles and Responsibilities (cont.)

Role	Possible Responsibilities
HIPAA Privacy Officer / Security Officer	<ul style="list-style-type: none">➤ Serve as compliance program administrators.➤ Conduct periodic HIPAA reviews & evaluate indiv. business unit compliance.➤ Partner with Corporate Compliance Officer and business unit liaisons to develop processes to identify and safeguard PHI and implement controls.➤ Provide subject matter expertise in the application of the HIPAA Privacy Rule and Security Rule.➤ Review new vendor relationships for HIPAA implications requiring Business Associate Agreements.➤ Serve as a member of HIPAA Incident Response Team to investigate and respond to suspected privacy and security breaches and incidents of non-compliance.➤ Create or review the appropriate training modules.➤ Respond to third-party inquiries related to disclosure of PHI



Compliance Program Roles and Responsibilities (cont.)

Role	Possible Responsibilities
Business Unit Management / HIPAA Liaisons	<ul style="list-style-type: none">➤ Be aware of the compliance program requirements, HIPAA requirements, and the business unit level impact.➤ Ensure the business unit adheres to the compliance program and HIPAA regulations.➤ Ensure efficient and effective management of HIPAA risks associated with business processes, products, and services.➤ Adhere to incident management protocol associated with suspected data privacy or security breaches.➤ Notify the Corporate Compliance and the HIPAA Privacy/Security Officer(s) of changes in existing processes, services, or vendor contracts that involve health information.➤ Consult with the Corporate Compliance Officer and the HIPAA Privacy/Security Officer(s) regarding new processes, services, or vendor contracts that involve health information so HIPAA impact can be determined prior to implementation.➤ Notify and consult with HIPAA Privacy Officer prior to the disclosure of PHI.➤ Review and communicate changes to HIPAA policies and procedures to employees.➤ Ensure all workforce members within business unit receive mandatory compliance training.



Compliance Program Roles and Responsibilities (cont.)

Role	Possible Responsibilities
Legal Department	<ul style="list-style-type: none">➤ Develop and update response policies and procedures for notification, litigation, or investigations related to data privacy and security breaches.➤ Monitor HIPAA or HITECH rule changes and notify the Compliance, Security, and Privacy Officers accordingly with any changes.➤ Develop policies and procedures for staff response to problems and breaches.➤ Review and update Business Associate Agreements.➤ Review all third-party contracts for PHI access or storage for the necessary data privacy and security measures.➤ Develop and maintain the HIPAA policies and procedures for the contractual relationship with the customer.



Compliance Program Roles and Responsibilities (cont.)

Role	Possible Responsibilities
Marketing / Product Development	<ul style="list-style-type: none">➤ Be prepared to respond to RFPs from healthcare payers and providers who seek assurance that the financial institution complies with HIPAA privacy and security regulations.➤ Ensure that new or enhanced products and services requiring compliance with HIPAA & HITECH are designed and promoted appropriately.➤ Review standing products for compliance issues; take appropriate steps to correct any deficiencies.➤ Work with Legal to review vendor relationships with remarketed products.



EHNAC

Electronic Healthcare Network Accreditation Commission

Questions to consider when evaluating HIPAA status (CE or BA?)

1. Does this service involve passing protected health information to a covered entity for reasons other than for payment posting?



2. Does this service involve modifying protected health information for a covered entity?

3. Does this service involve storing or archiving protected health information other than as part of processes utilized to process and post a payment?



EHNAC

Electronic Healthcare Network Accreditation Commission

Guidelines for implementation of policies/procedures for achieving compliance and mitigating risk: The Next Steps

- Determine eligible current or planned services and the financial institution's status as a covered entity or business associate under HIPAA and HITECH.
- Set-up the infrastructure to successfully achieve compliance. This task includes the selection of a corporate-level program sponsor as well as a privacy officer and a security officer. These roles may be assumed by one or more individuals.
- Conduct a risk analysis.
- Conduct a risk audit and identify controls or control gaps.



EHNAC

Electronic Healthcare Network Accreditation Commission

Guidelines for implementation of policies/procedures for achieving compliance and mitigating risk: The Next Steps (cont.)

- Review and update technology systems as needed.
- Develop a communications plan.
- Update workforce training.
- Consider data privacy and security accreditation or certification by an independent third-party such as EHNAC or HIMSS.



EHNAC

Electronic Healthcare Network Accreditation Commission

Sharon Klein, Esq. Pepper Hamilton LLP Regulation Overview (The Background)



EHNAC

Electronic Healthcare Network Accreditation Commission

Regulation Overview (The Background)

- HITECH: 2/09 as part of ARRA (\$20B allocated for
- HIT including EHR to reduce cost)
- Added accountability for financial institutions that provide medical lockboxes and other types of specialized services to healthcare providers and payers
- Many HITECH provisions modified and amplified the HIPAA provisions that affect financial institutions
- Financial institutions need to be knowledgeable about HITECH to:
 - assess whether the provisions impact current or planned services
 - guide development of reasonable internal policies, practices and procedures to help ensure compliance





EHNAC

Electronic Healthcare Network Accreditation Commission

Regulation Overview (The Background) (cont.)

- HIPAA – Enacted 1996 Includes the following provisions:
 - EDI Transactions (claim, eligibility, referrals, authorizations, remittance, etc.)
 - Privacy & Security Rules for: HC Payers, Providers & CH
 - 2001 MBP Hosts Roundtable to discuss implications of HIPAA on financial institutions
 - Further Research conducted by NACHA and ABA
 - 2004 NCVHS issues letter recommending that CE's that use financial institutions that directly access PHI must execute a BA until further clarification from HHS





EHNAC

Electronic Healthcare Network Accreditation Commission

Regulation Overview (The Background) (cont.)

- HIPAA Security/Privacy Rules:
 - Regulate the allowed uses and disclosures of PHI, which the law defines as individually identifiable health information in any form with minor exceptions
- BA defined:
 - A person or organization that performs an activity on behalf of a covered entity but is not part of the covered entity's workforce
 - Specifically addresses financial institutions as it includes entities that provide "...financial services to or for such covered entity ... where it involves the disclosure of individual identifiable health information





EHNAC

Electronic Healthcare Network Accreditation Commission

Implications for Financial Institutions

- Increased accountability
- Institutions must determine their compliance status as either a BA or CE, or as an entity solely performing payment processing and posting
- Meeting either definition of a BA or CE, an organization must develop and implement procedures and policies that ensure compliance with using and disclosing protected health information
- Under HITECH Act, BA is now held to many of the same requirements as a CE, especially in the areas of documenting and maintaining policies and procedures related to PHI and reporting information security breaches
- Financial institutions that are BA's/CE's must abide by regulations and guidance of the Office for Civil Rights (OCR)/DHHS



EHNAC

Electronic Healthcare Network Accreditation Commission

Jan Estep, President & CEO NACHA – The Electronic Payments Association

**Banking + Healthcare + ACH = The
NACHA Factor**



EHNAC

Electronic Healthcare Network Accreditation Commission

ACH – The Direct Network

Direct electronic movement of money
and related information



For consumers, businesses, and government



EHNAC

Electronic Healthcare Network Accreditation Commission

Brief Introduction to NACHA and the ACH Network

- NACHA is the private sector rule-making organization that administers the ACH Network.
- The ACH Network:
 - Facilitates global commerce by serving as a safe, efficient, ubiquitous and high-quality electronic payment system; it is best known for Direct Deposit and Direct Payment
 - Is accessible via more than 14,000 U.S. financial institutions
 - More than 19.4 billion ACH payments in 2010, moving \$31.7 trillion in value
 - Largest single user is the Federal government – 1.24 billion ACH payments in 2010, \$3.14 trillion in value
- Importantly, data transferred over this network is subject to privacy and security protections analogous to HIPAA requirements.

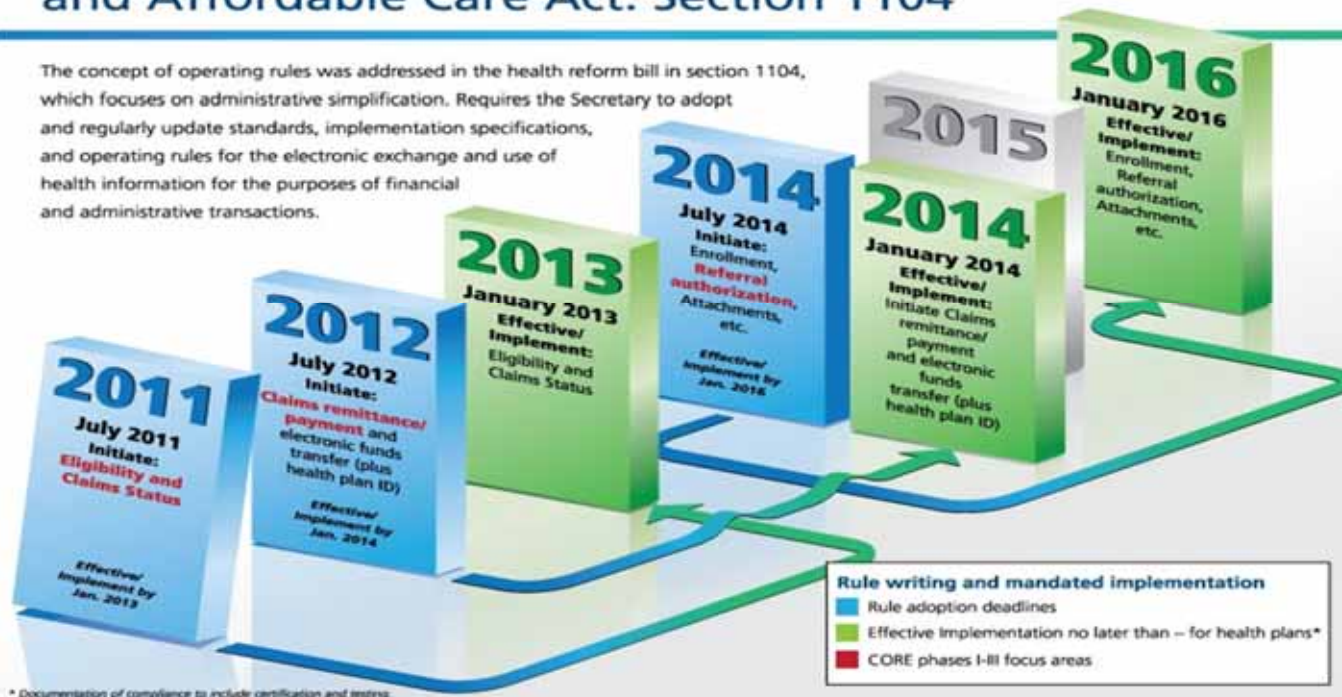


Health Reform Legislation Will Drastically Increase the Use of Electronic Health Care Payments

- For example, as of January 1, 2014, no Medicare payment may be made for any benefits delivered under Medicare Part A or Part B other than by EFT or an electronic remittance in a form specified in the payment/remittance advice HIPAA standard.
 - See Patient Protection and Affordable Care Act, Pub. L. 111-148 (PPACA), § 1104(d) (amending SSA § 1862(a)).

HR 3590 Patient Protection and Affordable Care Act: Section 1104

The concept of operating rules was addressed in the health reform bill in section 1104, which focuses on administrative simplification. Requires the Secretary to adopt and regularly update standards, implementation specifications, and operating rules for the electronic exchange and use of health information for the purposes of financial and administrative transactions.

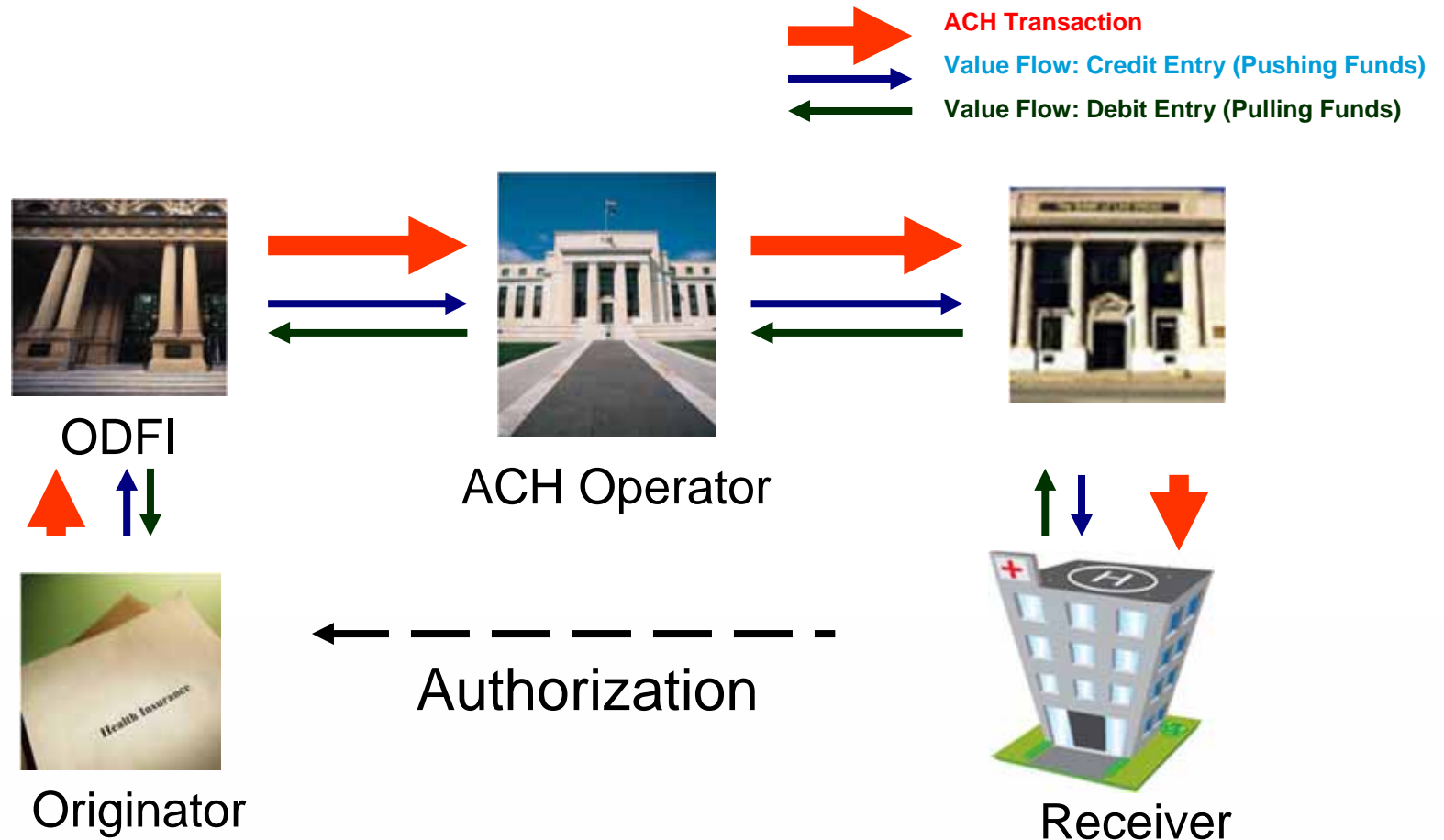




EHNAC

Electronic Healthcare Network Accreditation Commission

FIs can help health plans and providers of all types become **more** efficient by using electronic payments instead of checks.





Current System for EFT: Two B2B ACH Standards

- There are currently two ACH standards for EFT transactions between plans and providers: the “CCD+” standard and the “CTX” standard.
 - **CCD+** carries only the EFT payment and a re-association number over the ACH Network. It carries no PHI.
 - The ERA travels separately via some other electronic channel.
 - The provider must re-connect the remittances with the appropriate funds using the re-association number. This is typically a manual process.
 - ***NCVHS recently recommended the adoption of the CCD+ as the health care EFT standard transaction which health plans should utilize.***
 - **CTX** carries the EFT payment and the ERA together via ACH the ACH Network.
 - Re-association numbers are unnecessary when the CTX format is used, because the payment instructions (EFT) and payment information (ERA) move together over the ACH Network.
 - NCVHS stated that the CTX may be considered in the future as a health care EFT standard (see <http://www.ncvhs.hhs.gov/110217lt2.pdf>)



Standards and Rules work together to support healthcare

- Health plans use the ASC X12N 835 (Health care claim payment/remittance advice) for electronic remittance.
 - The 835 has two parts – the payment instructions, and the remittance advice. The payment instruction, which contains no PHI, may be used by a plan to initiate an EFT, but cannot accomplish a funds transfer – an ACH format is necessary for this.
 - Plans can specify a CCD+ or a CTX in the 835 payment instructions
 - When specifying a CCD+, the two component parts of the 835 are transmitted separately
- It is possible to transmit both EFT and ERA information together in a single transmission by specifying the CTX standard.
 - The 835 would be “enveloped” into the addenda records of the CTX.
 - Eliminates providers’ task of re-association
 - Eliminates time lapse in providers’ receipt of transactions



Current Overview of ACH Transaction Flow

- At a very high level, payment processing works as follows for both the CCD+ and the CTX transactions:
 - A large number of payment instructions (sometimes thousands) which may or may not be in ACH format are sent electronically by a health plan in a file to its ODFI.
 - A computer at the ODFI verifies that the data is in proper ACH format, converts it to proper ACH format if necessary, encrypts the data and forwards it to the ACH Operator.
 - A computer at the ACH Operator decrypts the information in order to syntactically validate the batch and sort the data into groups by RDFIs (providers' banks), re-encrypts the data and forwards it to the appropriate RDFI.
 - The RDFI's computer system decrypts the data in order to credit each EFT to the appropriate provider account.



FI's Ensure that Transmission of Information in Connection with all ACH Payments Is Secure

- Transmission of information in connection with ACH Payments is already subject to strict data security controls—separate and apart from HIPAA requirements.
 - NACHA Operating Rules Section 1.7 (“Secure Transmissions of ACH Information via Unsecured Electronic Networks”) requires that the banking information related to a payment transaction (which would include the ERA) must, at all times from the point of data entry and through the transmission, be either encrypted or transmitted via a secure session.
 - Financial institutions attest to compliance with this rule.
- Financial institutions transfer payment instructions to the ACH Operator using one of three methods (e.g., direct connections, FTP with SSL or Pretty Good Privacy (PGP) encryption or EPNAccess over the Internet.)
 - Each method of transmission to the ACH Operator uses standard encryption methodology for all files.



The ACH Network participants are closely audited by federal financial regulatory agencies.

- A variety of statutes, regulations and guidance requires that financial institutions maintain the confidentiality, integrity, and security of data entrusted to them for payment processing, i.e., FFIEC guidance.
- These laws are not specific to health care data, but the protections that are adopted by banks are applied broadly. As a result, health care data held by financial institutions is subject to protections – and both CCD+ and CTX transactions need to adhere to these regulations and protections.
- Similar to HIPAA, the framework requires that reasonable safeguards be adopted and does not dictate specific security choices. Financial institutions must implement a comprehensive written information security program that includes administrative, technical and physical safeguards appropriate to the size and complexity of the entity and the nature and scope of its activities.
 - Like HIPAA, the specific safeguards must be driven by a risk assessment.



General Privacy and Security Requirements Applicable to Financial Institutions

- Most FIs do not provide specialized services to healthcare entities, and do not routinely access PHI to perform services for those entities – they simply provide payment processing services.
 - Therefore, they are neither a BA or a CE.
- Nevertheless, by following financial services regulations, FIs will find that they have already embraced these types of required protections where reasonable and appropriate to support efficient payment processing and posting:
 - Technical and physical access controls for the building and the ACH operation areas
 - Intrusion monitoring
 - Authentication standards
 - Encryption
- Keep in mind that financial institutions are prohibited by law from using medical information to make credit decisions.



EHNAC

Electronic Healthcare Network Accreditation Commission

Impact of Healthcare Legislation on Financial Institutions



Level of impact varies depending on services offered by Financial Institutions to healthcare customers.



EHNAC

Electronic Healthcare Network Accreditation Commission

John Casillas, SVP, HIMSS Medical Banking Project

**The March Towards Electronic Business
Transformation in HC**



HIMSS Medical Banking Project

- The march towards electronic business transformation in healthcare
 - How it evolved in other industries and why its inevitable
 - SABRE, ASAP, others
 - The invaluable link to the banking system
 - Creating a strong ROI case for change
 - Key elements for administrative simplification
 - Health Payments Interoperability
- Creating cross-industry bridges
 - PHI flows and line of business impacts
 - Isolation of this critical nexus and examining it under the HIPAA lens
 - The promise of a new platform
 - Going mobile in healthcare
 - Online Banking



HIMSS Medical Banking Project cont.

➤ Potential future impacts

- The Identity Theft Arms Race: HIEs, HIX and the advent of repository-based structures

➤ Cross-industry regulatory impacts

- HIPAA / HITECH and beyond: FACTA, FIPS, FFIEC, and President Obama's new Cybersecurity Policy
- Are new services permissible National Bank activities?
 - What OCC and the Federal Reserve Board say
- A sustainable regulatory platform for change



EHNAC

Electronic Healthcare Network Accreditation Commission

Alberto Casas, Director, CitiBank EHNAC and Financial Institution Perspective

NOTICE: The information is not legal advice, and should not be construed or relied upon as such. In accepting these materials, you affirm that you are not relying upon these materials as a basis for any legal conclusions, and that you acknowledge that you should seek advice based on your particular circumstances from an independent legal counsel. While Citibank has endeavored to highlight some of the relevant sections of the law, it is not a full analysis of the matters presented, and Citibank makes no representation regarding the accuracy or completeness of the information presented herein.



EHNAC

Electronic Healthcare Network Accreditation Commission

Financial Institution Perspective:

- Financial Crisis has had a profound impact on how Financial Institutions manage risk and compliance. Unfortunately, HIPAA compliance is not top of mind for most:
 - Large Banks that have invested in medical banking services are engaged and aligned with changes in Privacy, Security and Transaction and Codes Set Changes.
 - For the most part, Mid-tier and Regional Banks represent largest exposure for compliance breaches.



EHNAC

Electronic Healthcare Network Accreditation Commission

Financial Institution Perspective:

- Why is there a lack of compliance and attention from Financial Institutions?
 - Lack of Education
 - Lack of Enforcement
 - Continued misinterpretation of relevance/applicability. For most banks, healthcare is not a familiar language
 - False notion that existing privacy and security standards exceed those of HIPAA and HITECH
 - For the most part Providers are not asking for or requiring proof of compliance beyond standard Business Associate agreement exchange
 - Some Financial Institutions continue to cite 1179 carve out



EHNAC

Electronic Healthcare Network Accreditation Commission

Financial Institution Perspective:

- Why should you care?
 - Doesn't matter how large or small you are or how many clients you support
 - 1179 carve out does not protect you
 - Financial penalties or broader enforcement are the least of your worries - social harm and resulting reputation damage are key concerns
 - PII and PHI distinctions
 - Emerging opportunities are afoot (2014 mandate, ACOs etc.)



Framework for Assessment and Compliance:

- Keep it simple - De-mystification of BA vs. Clearinghouse distinction
 - Requirements virtually same for privacy, security and notification (BA vs. Clearinghouse)
- How do I get started?
 - Assign internal champion with authority from Exec level
 - Self assessment
 - Identification of areas that support PHI
 - Functional and business partner engagement (Risk/Compliance, Legal, Operations, Sales/Marketing and Product)
 - Ongoing Organizational Alignment and Governance (Training, HIPAA Privacy Officer, Notification process etc.)
 - Seek external "Housekeeping Seal of Approval"



EHNAC

Electronic Healthcare Network Accreditation Commission

EHNAC - Financial Services Accreditation Program (FSAP)

- For banks and financial services firms engaged in healthcare.
- Ensures that organizations follow HIPAA security and privacy rules and meet a range of criteria specific to financial electronic health networks.
- Assures customers that their business partner follows industry-established standards for processing transactions involving protected health information.
- FSAP accreditation subprograms include:
 - FSAP-EHN
 - FSAP-Lockbox



EHNAC

Electronic Healthcare Network Accreditation Commission

Benefits of Accreditation

- Provides Competitive Advantage – Showcase Compliance With EHNAC Logo
- Value of a Good Nights Sleep
- Replicable Compliance Framework (Policies/Procedures/Governance)
- Ensures Implementation of Best Practices
- Ensures HIPAA/ARRA/HITECH as well as State of Maryland and NJ compliance requirements
- Provides compliment and support for other Audits (SAS 70 & Sarbanes-Oxley)
- Social Good



EHNAC

Electronic Healthcare Network Accreditation Commission

Discussion and Q&A