



**EHNAC**

Electronic Healthcare Network Accreditation Commission

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

Lee Barrett, Executive Director

May 15, 2011





# EHNAC

Electronic Healthcare Network Accreditation Commission

## Agenda for Session Today

- White Paper Objective/Key Findings
- Overview of Applicable Regulations (HIPAA & HITECH)
- Evolution of Financial Service & Resulting Rules & Regulations
- Implications for Financial Institutions





# EHNAC

Electronic Healthcare Network Accreditation Commission

## Agenda for Session Today (cont)



- Determining Your HIPAA Status
- Establishing Your Healthcare Privacy/Security Plan
- Compliance Program Roles & Responsibilities
- Next Steps for Your Organization



# EHNAC

Electronic Healthcare Network Accreditation Commission

White Paper Sponsored by:

***Electronic Healthcare Network Accreditation Commission***

[www.ehnac.org](http://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/>

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



***Workgroup for Electronic Data Interchange***

[www.wedi.org](http://www.wedi.org)

© 2010 Workgroup for Electronic Data Interchange, All Rights Reserved

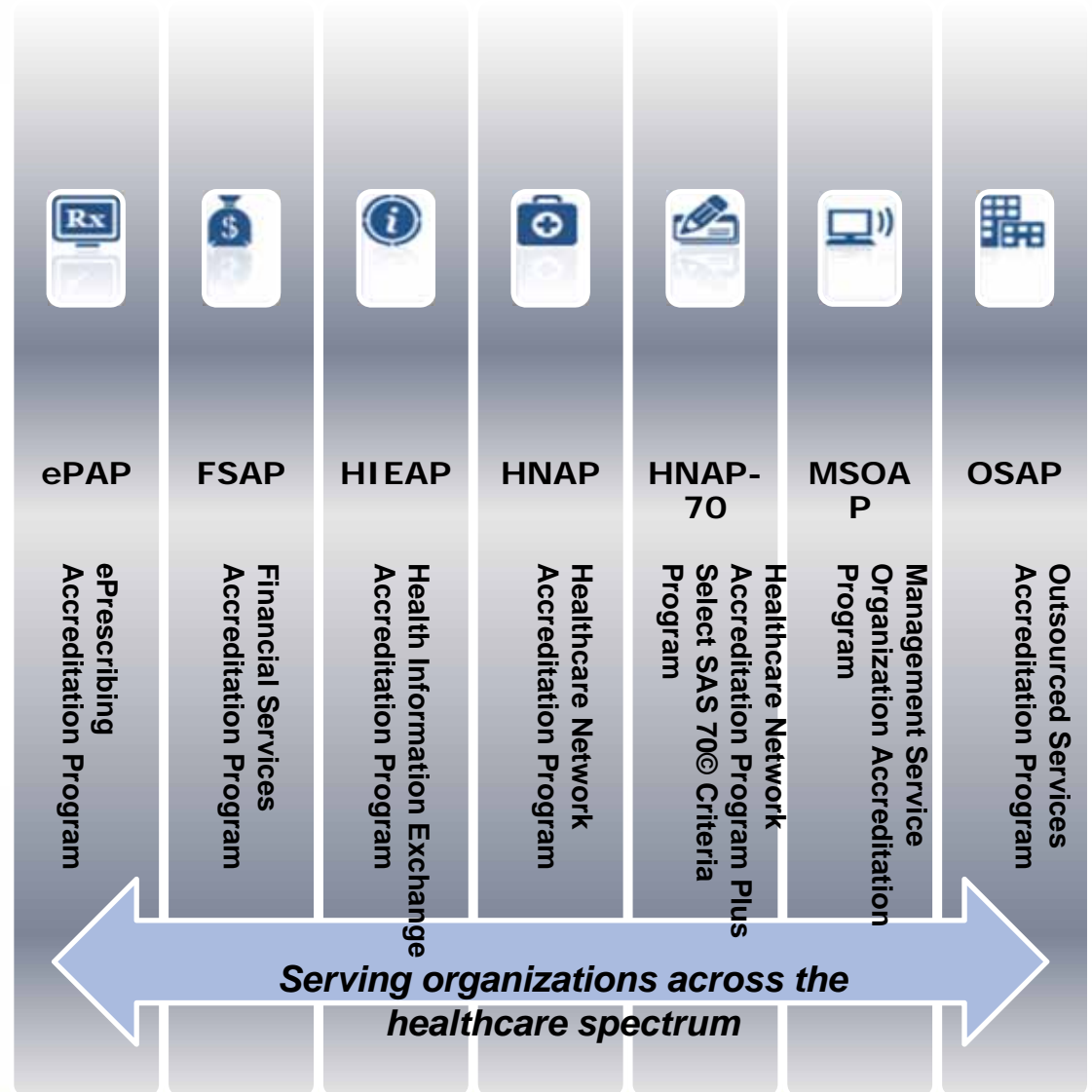


# EHNAC

Electronic Healthcare Network Accreditation Commission

## About EHNAC

- Established 1995
- Federally recognized SDO
- 501C6 Not-for-Profit
- Commission = 14 representing private & public sector stakeholders
- States of MD, NJ, UT and MN have regulations which mandate EHNAC accreditation for specific legislation





**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 financial institutions and their services for the healthcare sector.
  - Updated privacy and security rules
  - New breach reporting requirements
  - Tougher penalties



**EHNAC**

Electronic Healthcare Network Accreditation Commission

## White Paper Objectives & Key Findings (cont)



- Financial institutions 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



# EHNAC

Electronic Healthcare Network Accreditation Commission

## Regulation Overview (The Background)

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 that CE's that use financial institutions 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 ...





**EHNAC**

Electronic Healthcare Network Accreditation Commission

## Regulation Overview (The Background) (cont)

BA further defined:

- Regulation states that only a CE can disclose PHI to a BA
- The 1179 [42 U.S.C. 132d-8] exemption factor
  - The misperception demystified that HIPAA doesn't apply to any financial institutions





# EHNAC

Electronic Healthcare Network Accreditation Commission

## Regulation Overview (The Background) (cont)

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 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 to guide development of reasonable internal policies, practices and procedures to help ensure compliance





# EHNAC

Electronic Healthcare Network Accreditation Commission

## Regulation Overview (The Background) (cont)

HITECH modifies HIPAA in three key areas:

1. HITECH extends the Privacy Rule and Security Rule requirements directly to business associates.
2. HITECH adds strict breach reporting requirements.
3. HITECH toughens enforcement mechanisms and penalties.





**EHNAC**

Electronic Healthcare Network Accreditation Commission

## HIPAA Covered Entities

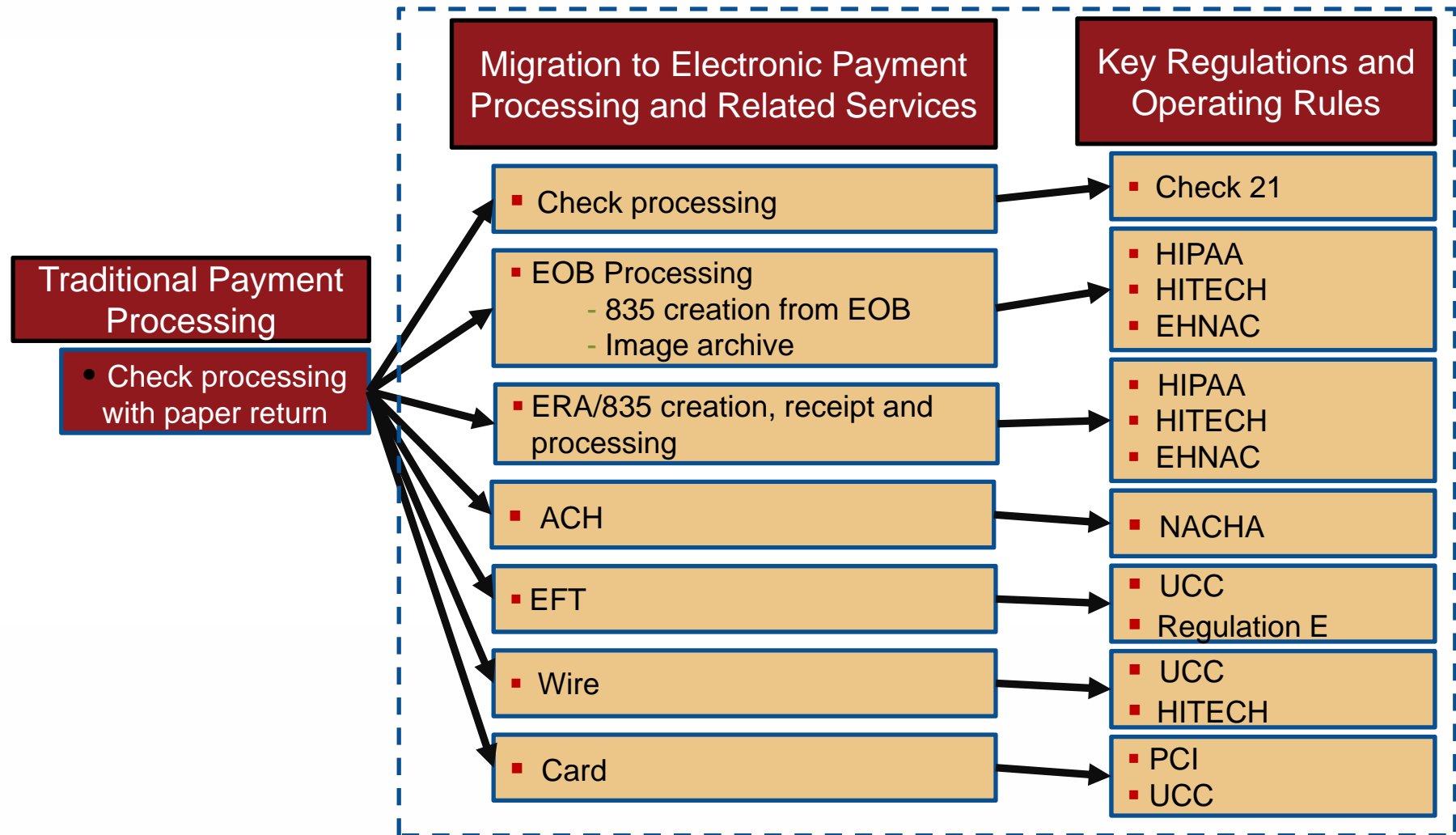
Covered Entity	Examples
Health Plan	Health insurance issuer, an MHO, Medicare, Medicaid
Healthcare Clearinghouse	A billing service, repricing company, community health information system, "value-added" network
Healthcare Provider	Includes facilities such as hospitals and clinics as well as individuals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

## **Implications for Financial Institutions**

- Increased accountability
- Institutions must determine their compliance status as either a BA or CE
- Meeting either definition 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 are now under the direct supervision of the Office for Civil Rights (OCR)/DHHS



**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?



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

3. Does this service involve storing or archiving protected health information?





# 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?



# EHNAC

Electronic Healthcare Network Accreditation Commission

## Compliance Program Roles and Responsibilities

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



# EHNAC

Electronic Healthcare Network Accreditation Commission

## Compliance Program Roles and Responsibilities (cont)

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



# EHNAC

Electronic Healthcare Network Accreditation Commission

## Compliance Program Roles and Responsibilities (cont)

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



# EHNAC

Electronic Healthcare Network Accreditation Commission

## Compliance Program Roles and Responsibilities (cont)

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



# EHNAC

Electronic Healthcare Network Accreditation Commission

## Compliance Program Roles and Responsibilities (cont)

Role	Possible Responsibilities
Marketing / Product Development	<ul style="list-style-type: none"><li>• 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.</li><li>• Ensure that new or enhanced products and services requiring compliance with HIPAA &amp; HITECH are designed and promoted appropriately.</li><li>• Review standing products for compliance issues; take appropriate steps to correct any deficiencies.</li><li>• Work with Legal to review vendor relationships with remarketed products.</li></ul>



# 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

# Discussion and Q&A