



e-business

# Fourth National HIPAA Summit

---

## HIPAA Case Study: Privacy Assessment and Remediation

Suzy Buckovich, JD, MPH  
IBM HIPAA National Practice  
sbuckovi@us.ibm.com

Greg Bard  NASCO  
NASCO Privacy and Security Project Manager  
gbard@nasco.com





e-business

# Agenda

- Background on NASCO**
- HIPAA Privacy Assessment Approach**
- Key Findings and Next Steps**
- Implementation Challenges**
- Lessons Learned**



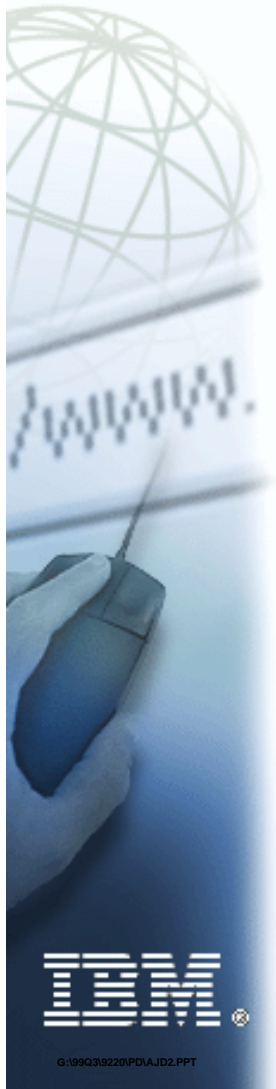


## Case Study:



### □ Background

- National Account Service Company LLC
- Transaction processing for 37 BCBS Plans, 6 million members
- 80 million claims per year
- Involves many IT vendors
- Data and application centers
- National Processing System (NPS)
- Tests applications and provides Customer Plan NPS training



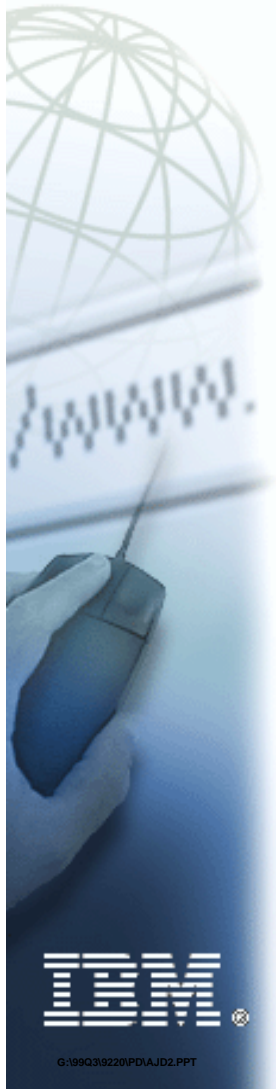


## Case Study:



### □ Privacy Challenges

- Complex Organization
- Relationships and Contracts with 37 BCBS Plans
- Involves many Business Associates, Vendors
- NASCO Wears Two Business Hats -- NASCO and Health Plan
- E-Business Initiatives (Healthcare Benefits Online Website)
- No In House Legal Department





e-business

# Privacy compliance required NASCO to assess its capability to support these areas

## Operational

- ↗ Understanding flow of PHI
- ↗ Uses and disclosures
- ↗ Workforce training
- ↗ Termination procedures
- ↗ Designated privacy responsibility

Privacy  
Requirements

## Policy and Procedures

- ↗ Corporate privacy policy
- ↗ Departmental procedures
- ↗ Complaints and sanctions
- ↗ Internal books
- ↗ PHI storage

## Individual Rights Processes

- ↗ Access, Copy
- ↗ Amend
- ↗ Accounting of disclosures
- ↗ Tracking requests, actions
- ↗ Authorizations
- ↗ System impact

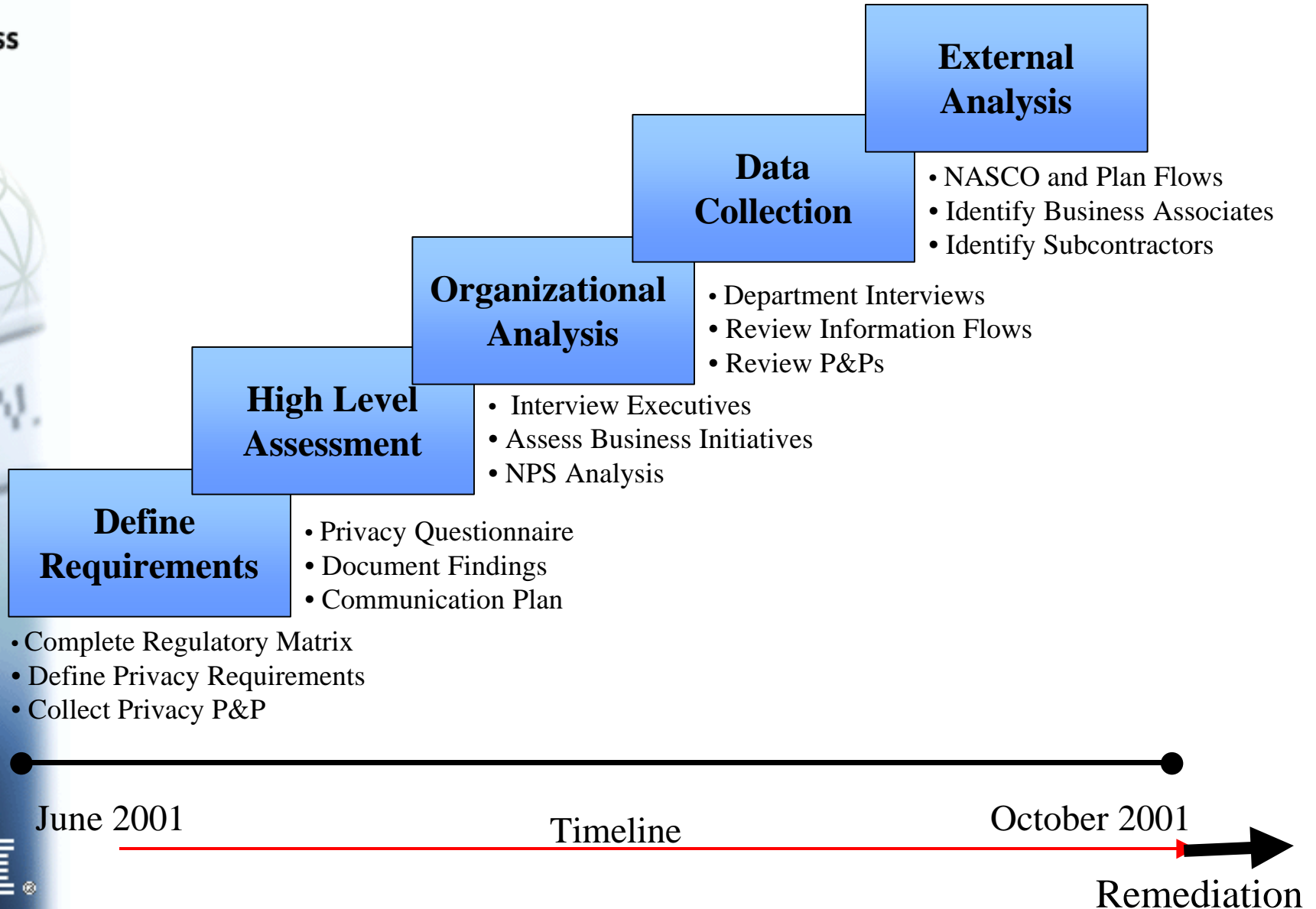


IBM



e-business

# Privacy Assessment Approach

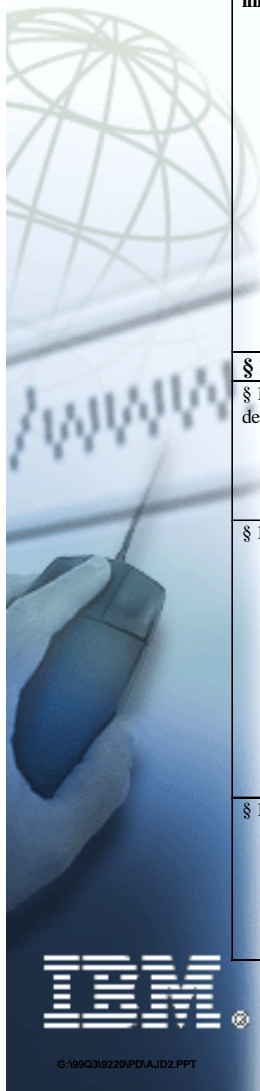




# Privacy Regulatory Grid

e-business

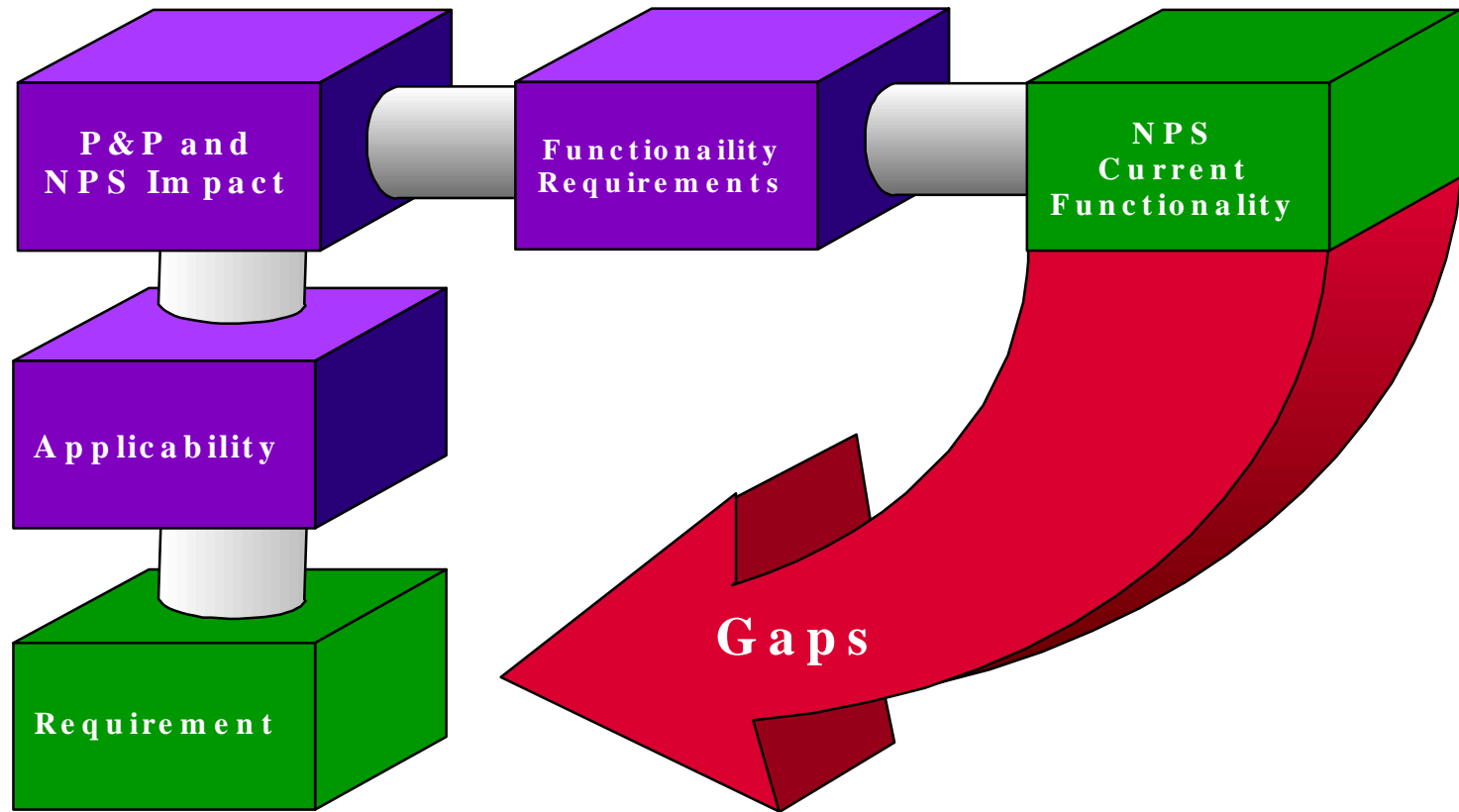
Privacy Regulation Requirement and Citation	Description of Requirement	NASCO's Response If Applicable, Include Policy/Procedure Link
<p>§ 164.528 Accounting of disclosures of protected health information.</p>	<p>An individual has the right to <u>receive an accounting of the disclosures of PHI made by the covered entity in the six years</u> prior to the request except for disclosures: (1) for payment treatment and operations, (2) to the individual, (3) for the facility's directory or to person's involved in the individual's care, (4) for national security or intelligence purposes, (5) to correctional institutions or law enforcement officials, (6) prior to the compliance date.</p> <p>Covered Entities must provide: One free accounting per year; additional copies for a reasonable fee Within 60 days of request (90 with extension) The covered entity must provide a written accounting of disclosures that for each disclosure includes the date of the disclosure, the person to whom the information was disclosed, a brief description of the information disclosed or in lieu of the summary, a copy of the authorization or request for disclosure. Business Associates must sign a contract that includes a provision that they will provide an accounting of disclosures (other than for treatment, payment, and health care operations)</p>	<p>Does NASCO have documentation of the purposes of their disclosures? <b>No</b></p> <p>Is there a PHI disclosure log? <b>No</b> (If "no" stop) Does it include: disclosure date person disclosed to description of disclosed information copy of the authorization or disclosure request? Does it cover 6 years? (y/n) Does your operations support disclosure log retrieval and dissemination within 60 days? (y/n) Do you document or track through other mechanisms the accounting of disclosures? <b>No</b></p>
<p><b>§ 164.530 Administrative requirements</b></p>		
<p>§ 164.530 (a) Personnel designations.</p>	<p>Covered Entity must Designate a Privacy Official responsible for the development and implementation of the policies and procedures of the entity AND a contact person or office to receive complaints provide further information about the covered entities privacy practices.</p>	<p>Is there a Privacy Official? <b>Yes</b> Is this privacy official responsible for the privacy policies and practices? <b>Yes</b> Is there a contact office or person for complaints and to provide information regarding privacy practices at NASCO? <b>Yes</b></p>
<p>§ 164.530 (b) Training</p>	<p>A covered entity must train members of its workforce about the entity's policies and procedures for protected health information and document that training has been provided. The entity may demonstrate compliance by simply documenting attendance at the training; for example, by means of sign-in sheets or notations in personnel records. Training must be completed by the following dates: For each member of the covered entity's workforce, by no later than the compliance date for the covered entity; and Thereafter, for each new member of the workforce, within a reasonable period of time following the date of hire; and Within a reasonable period of time after a material change in one of the entity's privacy policies or procedure becomes effective</p>	<p>Do you have a training program concerning PHI for your workforce? <b>No</b> If Yes, is this training documented? (e.g., signed statements by workforce) Are the training materials updated on a regular basis? Are there ongoing re-education to address changes as they occur?</p>
<p>§ 164.530 (c) Safeguards</p>	<p>A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of PHI and reasonably safeguard PHI from any intentional or unintentional use or disclosure, or violation of the requirements of the regulation. For PHI in electronic form, <u>compliance would be required with both the privacy standard and the proposed HIPAA Security Standards</u> related to safeguarding the privacy and integrity of health information</p>	<p>Do you have appropriate (1) administrative (2) technical (3) and physical safeguards in place to protect PHI? <b>No, only limited and very informal safeguards</b></p>





e-business

# NPS System Analysis



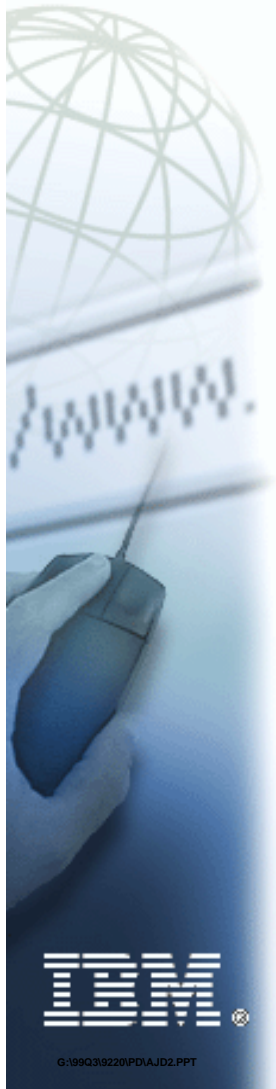


DESCRIPTION	APPLICABILITY				P&P IMPACT	Front End: Membership, Provider, and Pricing Benefit Adm: Claims Adjudication, Medical Policy, Benefit Determination Backend Financials: Claim Check, Utilization Review, COB, Payment					Functionality	NASCO'S Capability to Support Individual Rights			
	BA	CH (BA)	CH not a (BA)	HP		D	F	B	B	F	R	C	S	System Requirements	Current Capability
					e v e l o p P & P	r o n e t E n d m	B e n e f i t A d m	B e n e f i t A d m	F e n d i n g	R e q u i r e m e n t s					
<b>Individual Rights</b>															
<b>I. Right to Access/Copy</b> Individuals have the right of access to inspect and obtain a copy of their protected health information in a designated record set. Covered entities may deny this request based upon regulatory exception	X	X	X	X	YES	X	X	X	X	X			> System must include PHI identifier search capability (e.g. name of individual or some identifying number, symbol, or other identifier assigned to an individual >If healthplan requests dependent level search, s	>Subscriber ID search capability >SSN search capability >Membership system includes qualifier search (e.g. sex and relationship) for dependents >No COB or other PHI qualifier searches	> NASCO - <b>NO</b> NPS has a subscriber search function; <b>YES</b> , there is a gap if the search is requesting a dependent level > NPS to support HP - <b>Same as above</b>





e-business



# HIPAA Privacy Assessment

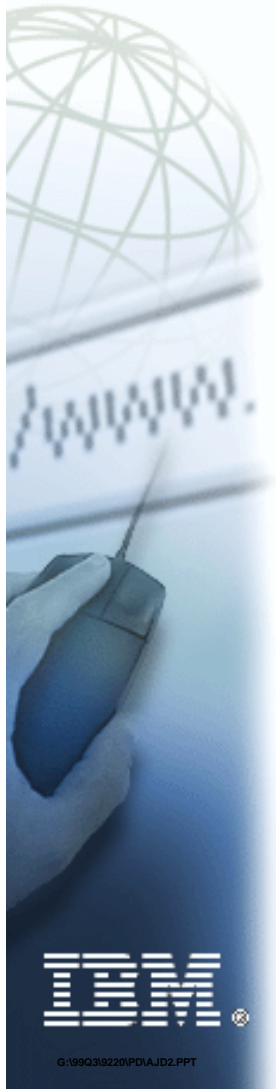
## Key Findings





# HIPAA Privacy Assessment: Key Findings

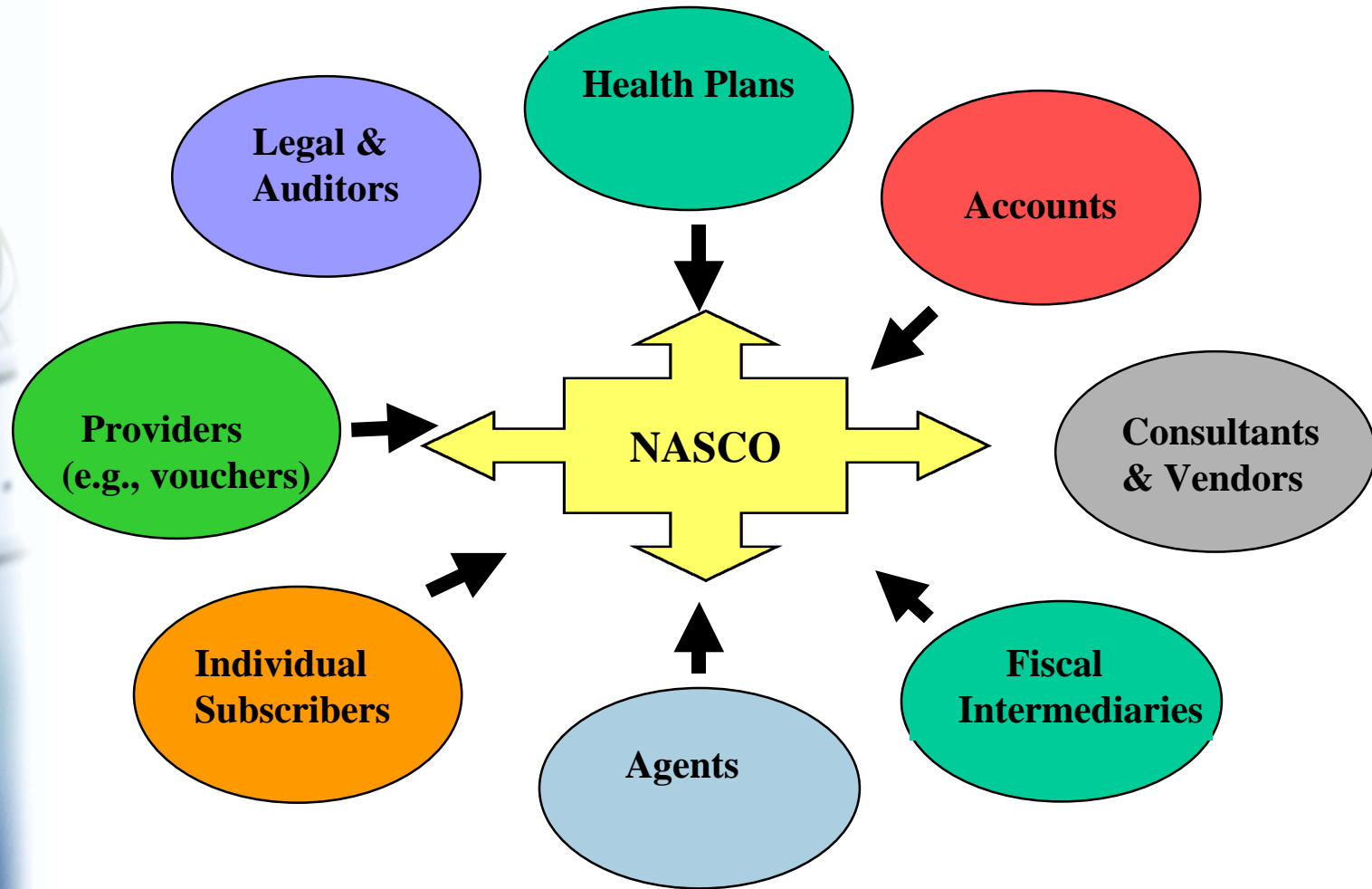
- Lack of centralized responsibility to track contracts, business associate relationships, permission letters**
- Lack of formalized process for releasing PHI**
- Use of PHI in training materials**
- Some NASCO associates have access to PHI that is not necessary to perform their jobs**
- Informal policies and procedures exist surrounding the uses and disclosures of protected health information**
- Lack of process in place to track disclosures of PHI**





e-business

# Findings: PHI Sharing



*Important to document to identify PHI touch points*

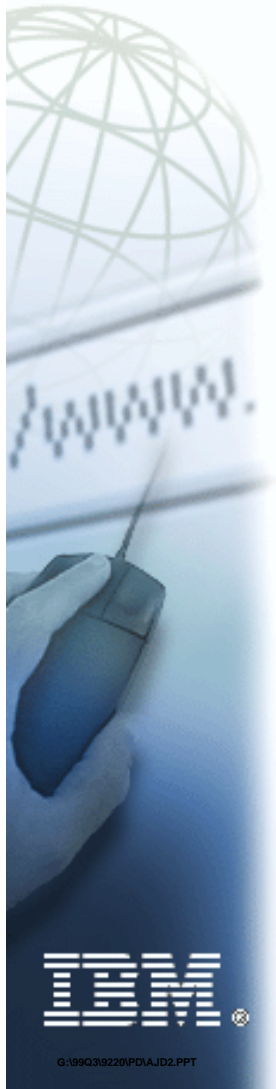
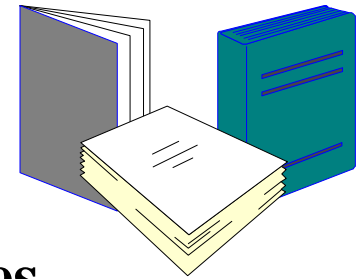




e-business

# Findings: Policies and Procedures

- Existing confidentiality statements
- Informal authorization procedures
- Lack of formal, written privacy policies and procedures for protecting PHI (fax, email, training manuals, etc.)
- Lack of tracking procedures to document disclosures





e-business

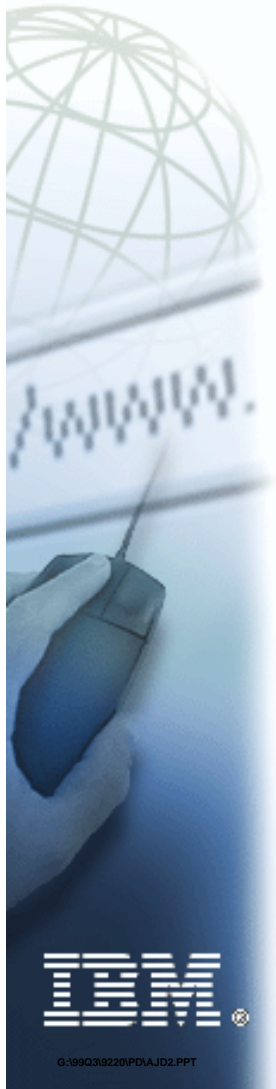
# Findings: NPS Analysis

<b>FINDINGS</b>	<b>GAP</b>
Individual Rights	Gap (Confidential Communication)
Storage	No Gap
Preemption	TBD
Membership	Gap (Confidential Communication)





e-business



# **HIPAA Privacy Assessment**

## **Key Next Steps**

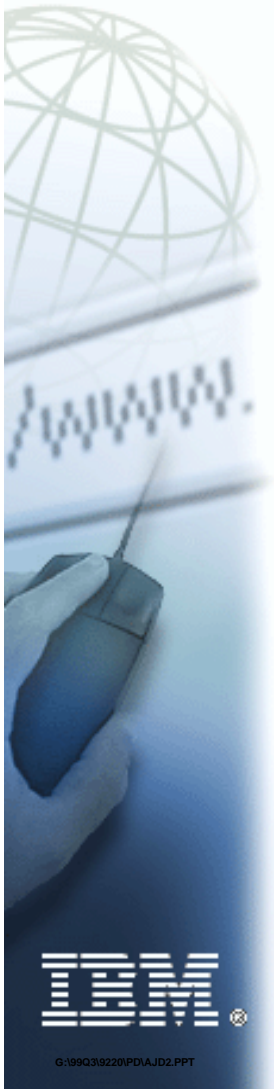
### **A Roadmap to Meet Privacy Requirements**





# HIPAA Privacy Assessment: Key Next Steps

- Designate a person or department to track existing contracts, business associate relationships
- Formalize release of information process (P&P)
- Develop processes to support individual rights (P&P)
- Develop privacy policy and training program (P&P)
- Review HCBO website (privacy statement, features, branding, etc.)
- Develop implementation project plan







e-business

# Contracts/Agreements

- Centralize responsibility for identifying and tracking Business Associates**
- Develop strategy for contract coordination and management**
- Negotiate Business Associate Contracts**

Name of Entity	Function Performed	Involves Protected Health Information? Y/N	Contract Required Y/N	Does a contract exist? Y/N	Is Contract Signed? Y/N  Date Signed
1. XXXVendor	Print checks, EOBs, vouchers for NASCO; host website (VISIONS) for health plans	Yes Vendor employees access/view/print PHI	Yes	Yes	Yes 02/26/02





e-business

# Track Accounting of Disclosures

Requester	Disclosed PHI	Date	Time Period for request (last 6 years Y/N)	Name and address of person receiving PHI	Description of purpose	Multiple Disclosures
Subject Individual	EOB	May 2, 2000	April 5, 1998 (within 6 years)	John Smith Police Officer	Legal Proceeding	No

- **Develop processes to implement the individual's right to receive an accounting of disclosures**

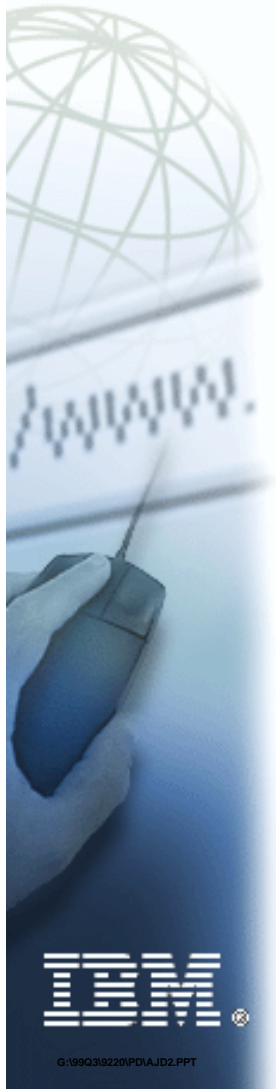
- identify disclosures outside of treatment, payment, health care operations
- create logging mechanism (could manual log) for those disclosures outside of treatment, payment, health care operations
- designate person responsible for responding to this request
- respond (approve/deny) in a timely manner (develop response form)
- maintain documentation for 6 years





# Support Individual Rights: Access/Copy and Amend


- Develop policy and procedures to receive requests from covered entities and individuals (including schedule and costs), access process, approve and/or deny process, amend process**
- Document and log requests, actions, information copied**
- Designate NASCO contact person to process requests**
- Maintain documentation for 6 years**

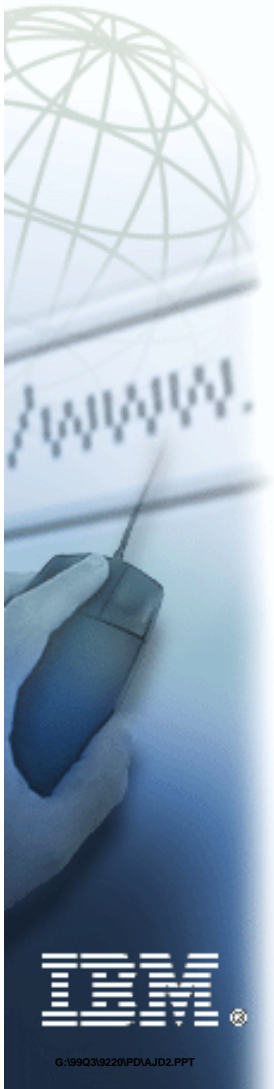




e-business

# Policies and Procedures

- **Develop privacy mission statement**
  - *“NASCO is committed to protecting the privacy of health information”*
  - *Part of Branding Initiative*
- **Develop written privacy policies and procedures for protecting PHI (fax, email, training manuals, etc.)**
- **Develop formal complaint processes and sanction policies**
- **Formalize release of PHI form**
- **Develop privacy manual (due diligence document)** 





e-business

# Summary of Next Steps: Implementation Plan

Next Steps	Owner/Team	Estimated Completion
1. Coordination of tracking contracts – Business Associate, Trading Partner, Chain of Trust	XXX	2002
2. Develop strategy for training materials	XXX	2002
3. Develop privacy policies and procedures	XXX	03/31/02
4. Develop standard authorization forms and procedures for outside disclosures	XXX	03/31/02
5. Develop policy and procedure to support the three individual rights as a Business Associate: Access/Copy, Amend, Accounting of Disclosures	XXX	03/31/02
6. Coordinate privacy workgroup to facilitate discussion of HIPAA related to ongoing business initiatives (e.g. E-Business Workgroup Meeting)	XXX	04/14/03
7. Develop ongoing privacy awareness education program	XXX	04/14/03

Each has its own project plan with milestones





e-business

# Summary of Next Steps: Implementation Plan

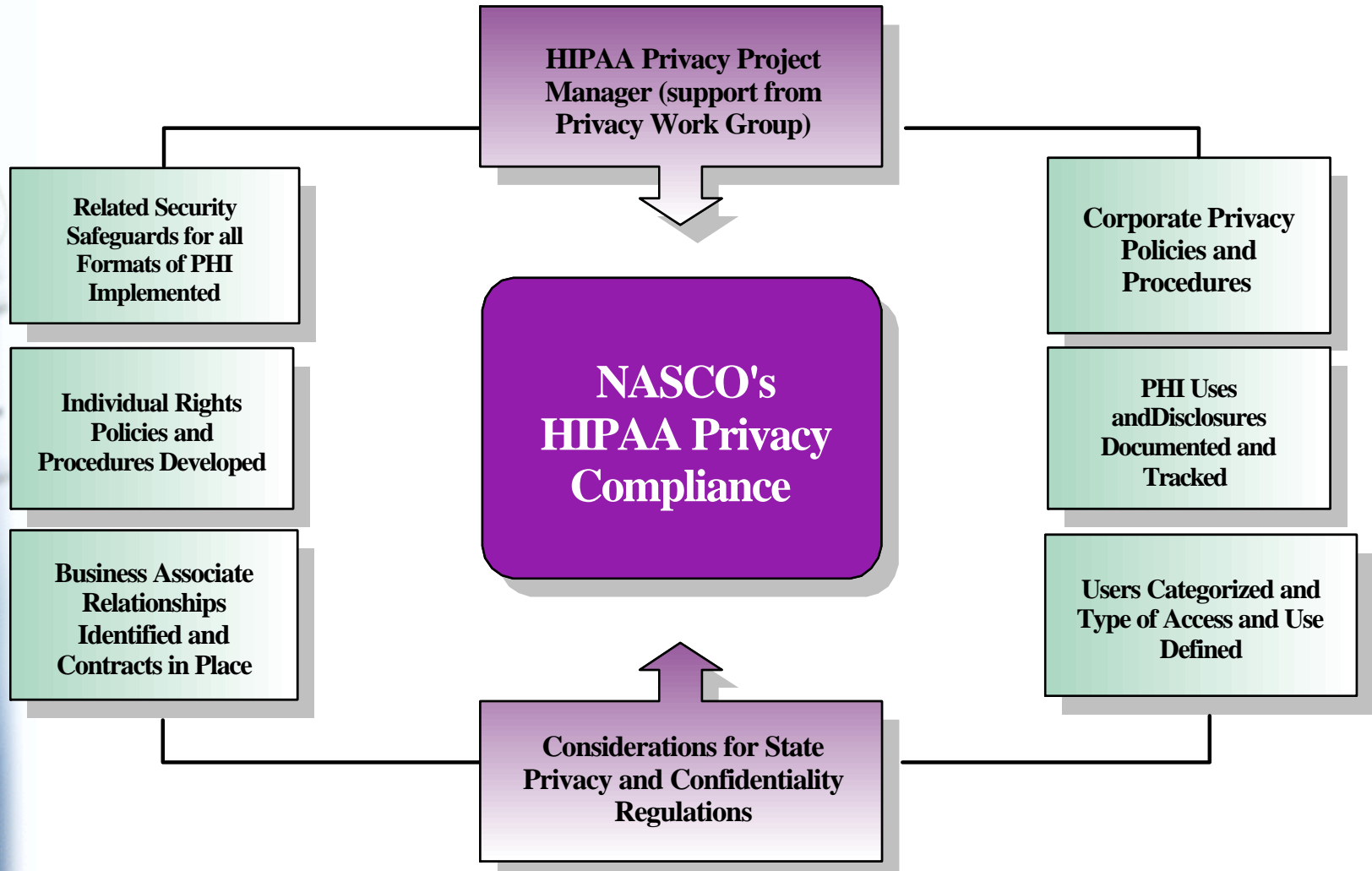
Next Steps	Owner/Team	Estimated Completion
8. Preemption – Assign point of contact	xxx	TBD – Will be driven based on Plan requirements
9. Satisfy storage requirements – develop procedures for documentation storage requirements ( <i>policy and procedure</i> )	xxx	03/31/02
10. Support Individual Right of Confidential Communication	xxx	TBD
11. Support Revocation of Authorization – Manual Procedure ( <i>policy and procedure</i> )	xxx	03/31/02





e-business

# Privacy Implemented at NASCO



*This depicts NASCO's due diligence*





# Privacy Implementation Challenges

e-business

## ■ Understanding Uses and Disclosures

- ✘ Identify Protected Health Information
- ✘ Documenting Information Flows
- ✘ Understand Permitted and Required
- ✘ Train Workforce

## ■ Document Management

- ✘ Consents, Authorizations, Opt Outs
- ✘ Privacy Policies, Notices of Practices
- ✘ Track Requests to Exercise Rights
- ✘ Track Individual Appeals, Disputes
- ✘ Maintain Accounting of Disclosures

## ■ Minimum Necessary

- ✘ Determining Need to Know
- ✘ Use and Disclosure Procedures
- ✘ Defining Routine and Recurring
- ✘ Defining Individual Criteria
- ✘ Training Workforce

## ■ Individual Rights

- ✘ Assess System Functionality
- ✘ Tracking Requests, Denials, Reasons
- ✘ Tracking Revocations (manual?)

## ■ Business Associate (BA) Contracts

- ✘ Understanding Information Sharing Practices and Procedures
- ✘ Identifying All Business Associates
- ✘ Identifying Your Own Entity as a BA
- ✘ Negotiating/Renegotiating Contracts
- ✘ Contract Management

## ■ Preemption

- ✘ Identifying Contrary and More Stringent Laws
- ✘ Existing Patchwork of Privacy Laws
- ✘ Multi State and National Locations

## ■ Administrative Safeguards

- ✘ Intersection of Privacy and Security Controls
- ✘ Identifying Need for Audit Trails

## ■ Compliance

- ✘ Internal Audit
- ✘ Audit Controls
- ✘ Monitoring



IBM





e-business

# Lessons Learned

- Confirm what you are under the regulation**
- Privacy is not just about policy and procedures -  
- it also impacts systems**
- Understand and document PHI business process  
flows (Sr. management verification and  
consensus)**
- Communication is key**
- Need for coordinated, organized and structured  
approach**
- Use of data collection tools**



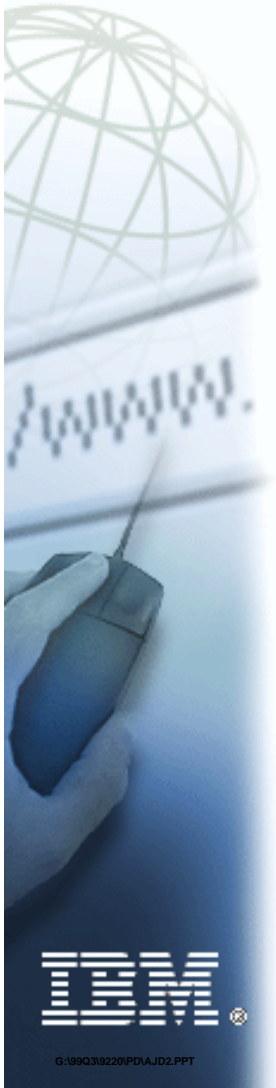
IBM



e-business

# Lessons Learned

- Importance of identifying Business Associates (and obtaining approval)**
- Don't wait to develop strategy for contract negotiations**
- Critical to understand HIPAA impacts on future business initiatives**
- Important to obtain assistance from HR department (P&P, training)**
- Involve legal counsel as appropriate**
- Document, document, document (due diligence)**



IBM



e-business

# Questions?

