Minimum Necessary: What is Enough?

Developing Policies and Procedures: Approach and Lessons Learned

Sixth National HIPAA Summit
March 28, 2003

Joan Furman, MBA, MSA
Privacy Project Director, Empire BCBS
joan.furman@empireblue.com

Suzy Buckovich, JD, MPH
Managing Consultant, IBM
sbuckovi@us.ibm.com

Empire BLUECROSS BLUESHIELD

Presentation Objectives

- Present a case study of one approach to minimum necessary
- Provide tools to collect disclosure, use and request information
- Provide examples of minimum necessary policy and procedures

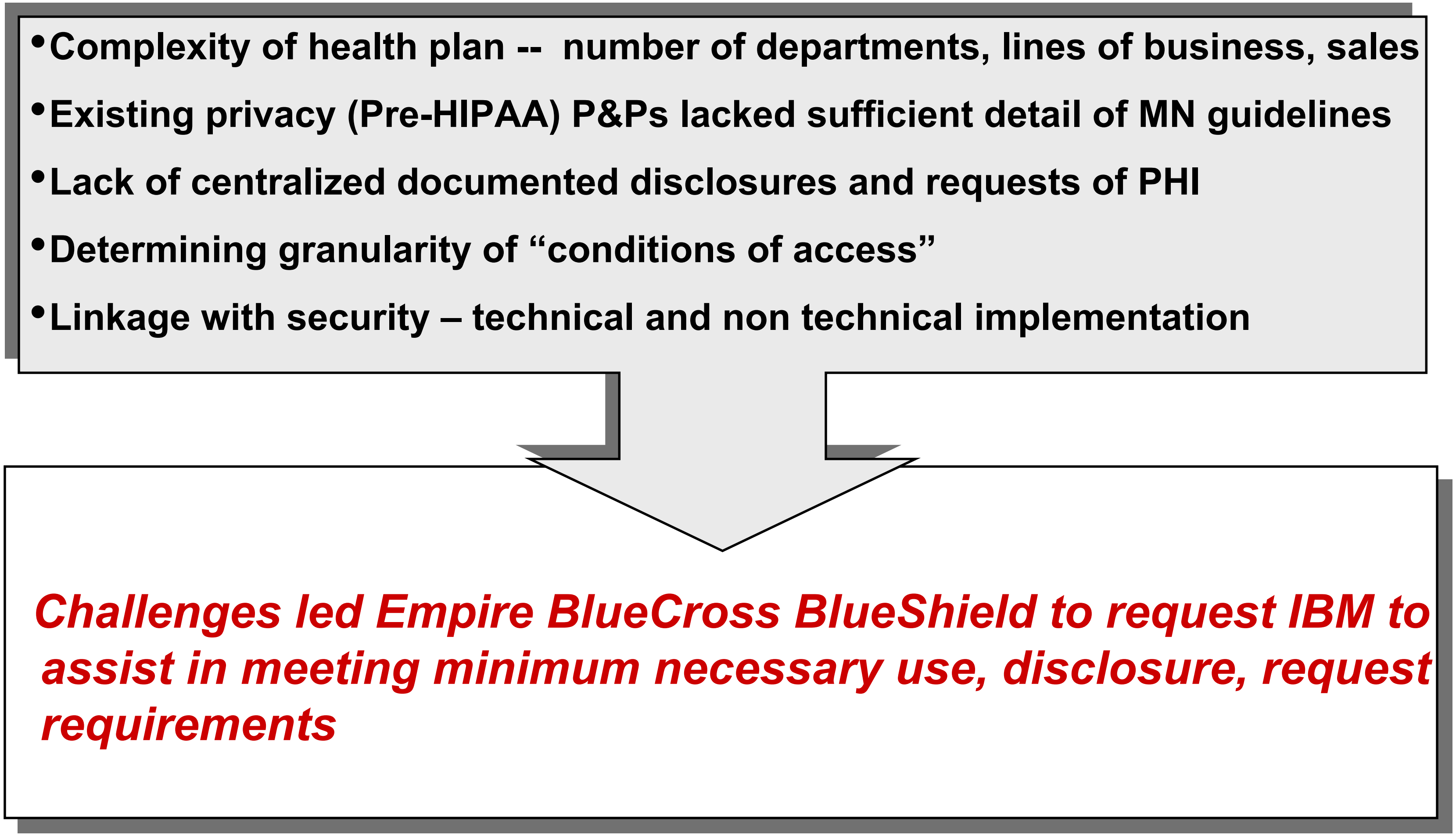
Agenda

- Background
- Minimum Necessary Project Approach and Tools
- Policy and Standard Operating Procedures
- Compliance Monitoring
- Lessons Learned

Background – Empire BlueCross BlueShield

- Large health plan with 4.6 million members
- 6,000 employees
- Products
  - Traditional indemnity plans
  - Preferred provider plans (PPO)
  - Managed Plans (HMO/POS)
  - Medicare supplemental plans
  - Medicare fee-for-service as Medicare intermediary
- 120 functional units (cost centers)
- Customer service websites (member, provider, GBA, broker)
- Sept. 11 impact (different locations)
- 2 major IT platforms (local and national accounts)

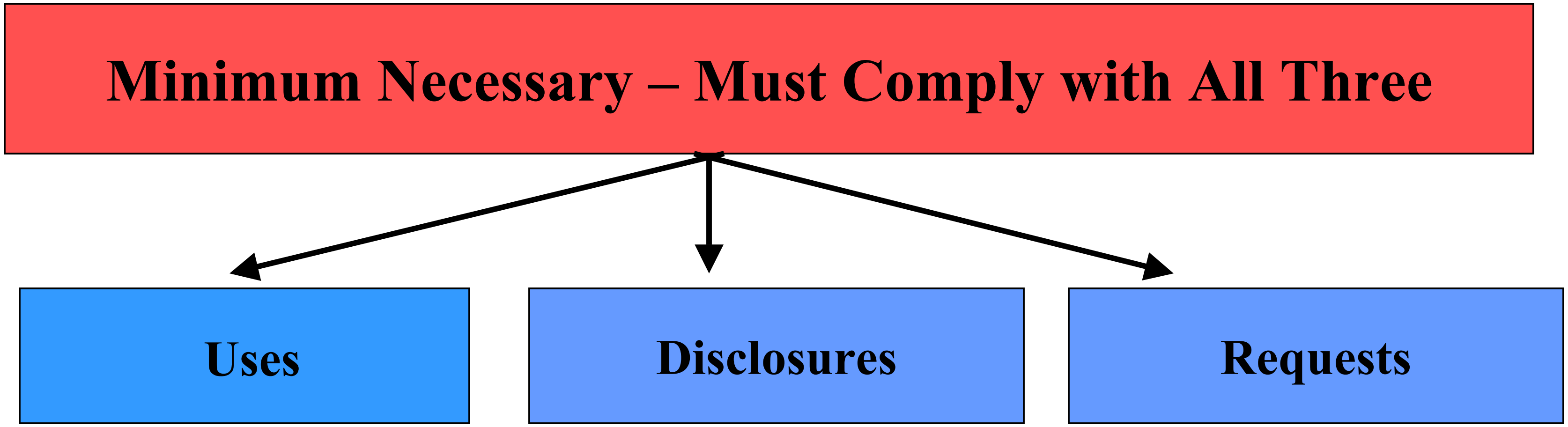
Minimum Necessary Challenges



- Complexity of health plan -- number of departments, lines of business, sales
- Existing privacy (Pre-HIPAA) P&Ps lacked sufficient detail of MN guidelines
- Lack of centralized documented disclosures and requests of PHI
- Determining granularity of “conditions of access”
- Linkage with security – technical and non technical implementation

Challenges led Empire BlueCross BlueShield to request IBM to assist in meeting minimum necessary use, disclosure, request requirements

Minimum Necessary Regulatory Requirements



Minimum Necessary – Must Comply with All Three

Uses

Disclosures

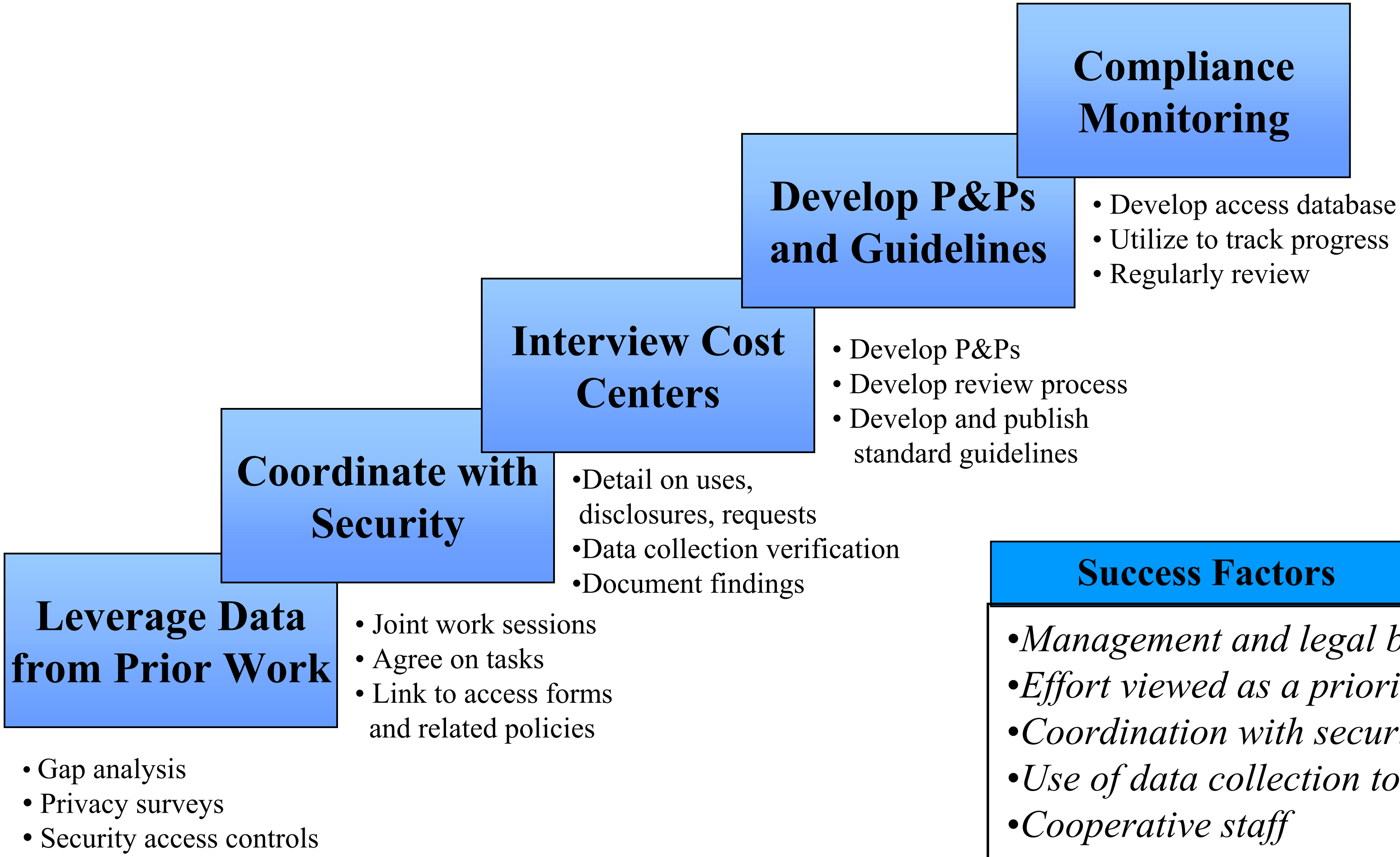
Requests

- •Develop Corporate P&Ps
- •Identify persons or classes of persons who need access to PHI to perform their jobs
- •Categorize PHI they need access to perform their jobs
- •Identify condition of access

- •Develop Corporate P&Ps
- •Identify disclosures of PHI
- •Review criteria for non routine
- •Develop non routine disclosure log
- •Identify accounting of disclosure items
- •Develop "standard guidelines" for routine disclosures

- •Develop Corporate P&Ps
- •Identify requests of PHI
- •Develop review process for non routine
- •Develop non routine request log
- •Develop "standard guidelines" for routine requests

Minimum Necessary Project Approach



Leverage Data from Prior Work

- Gap analysis
- Privacy surveys
- Security access controls

Coordinate with Security

- Joint work sessions
- Agree on tasks
- Link to access forms and related policies

Interview Cost Centers

- Detail on uses, disclosures, requests
- Data collection verification
- Document findings

Develop P&Ps and Guidelines

- Develop P&Ps
- Develop review process
- Develop and publish standard guidelines

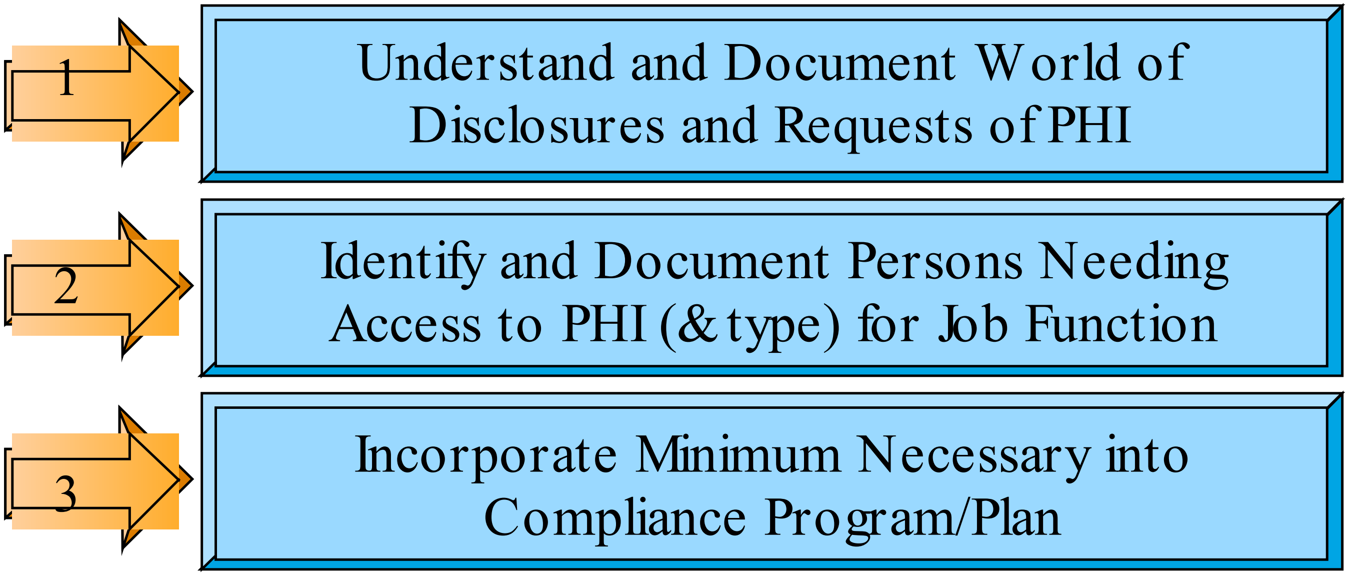
Compliance Monitoring

- Develop access database
- Utilize to track progress
- Regularly review

Success Factors

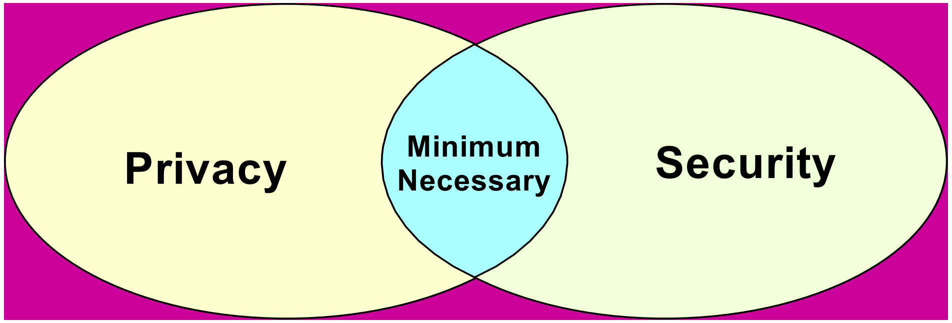
- *Management and legal buy-in*
- *Effort viewed as a priority*
- *Coordination with security*
- *Use of data collection tools*
- *Cooperative staff*

Minimum Necessary Project Objectives



1. Understand and Document World of Disclosures and Requests of PHI
2. Identify and Document Persons Needing Access to PHI (& type) for Job Function
3. Incorporate Minimum Necessary into Compliance Program/Plan

First Step -- Privacy and Security Coordination is Critical
Work Together to Understand Interdependencies

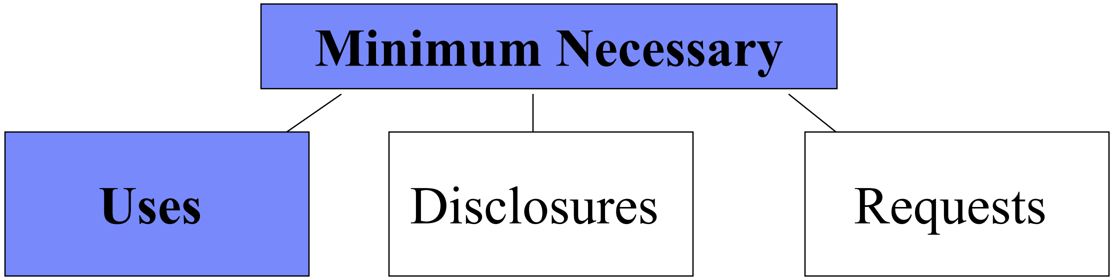

Privacy

Minimum Necessary

Security

Identify Persons Needing Access to PHI	Provide Reports on Persons with Actual Access
Identify Categories of PHI Needing Access to for Job	Assist in Locating PHI; Defining Subsystems
Identify and Document Condition of Access	Define Condition; Define System Capabilities
Implement Minimum Necessary Policy and SOP	Link to Forms & Procedures Implement Technical Controls

Final HIPAA Security Standards Link to Minimum Necessary

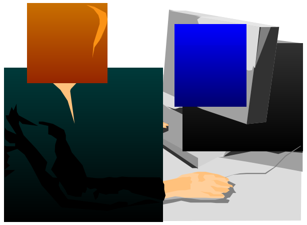


Privacy defines who gets access to what PHI and Security implements those policies

- **Workforce Security Standard**
  - assurance that all personnel with access to electronic protected health information have the required access authority as well as appropriate clearances.
- **Information Access Management Standard**
  - Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements
- **Access Control Standard**
  - Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights

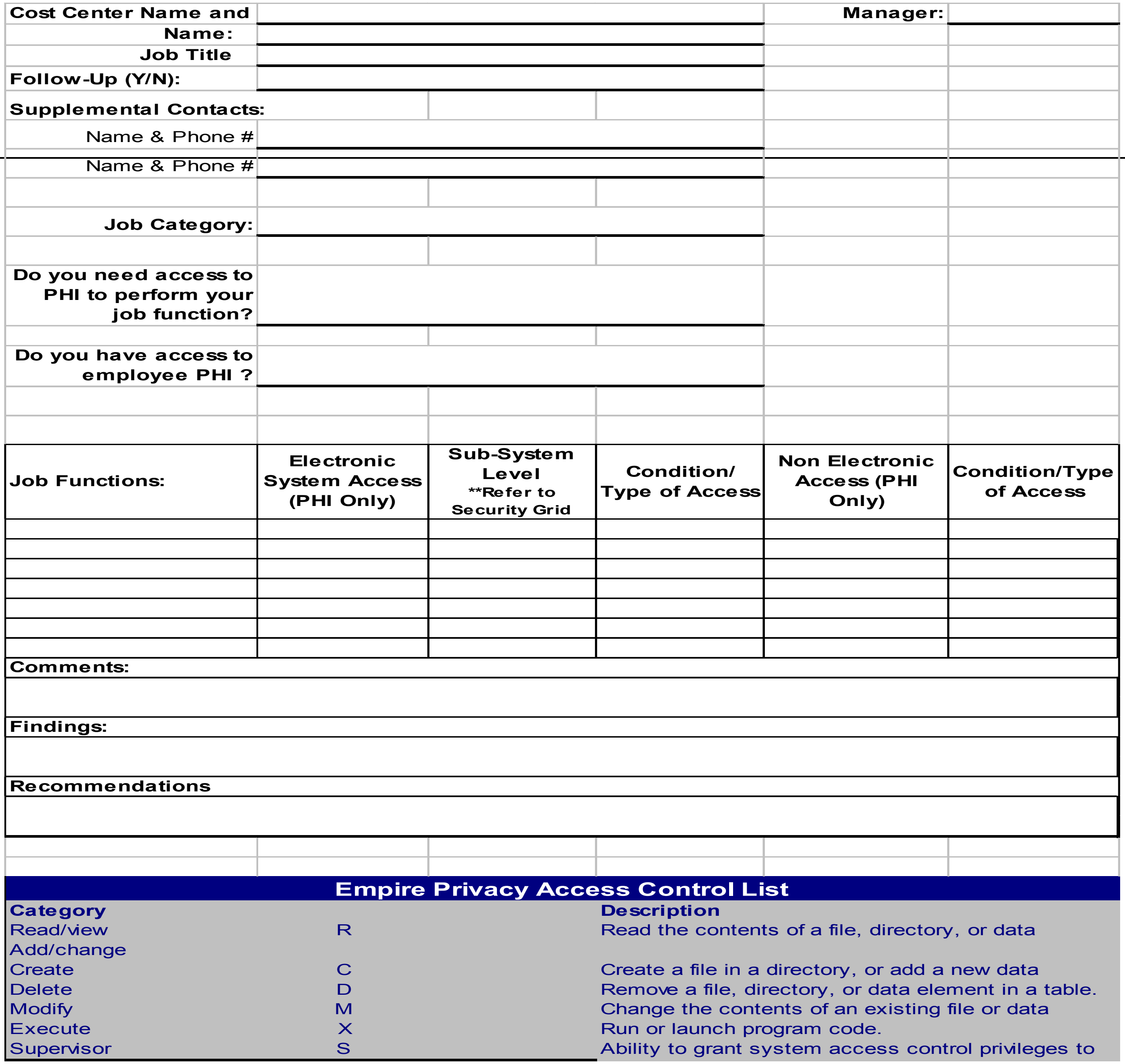
Minimum Necessary Interview Process

- Questioned need for access to PHI (not focus on “have access” to PHI)
- Collected detail down to the PHI data element where appropriate
- Asked owners of disclosures and requests to ensure minimum necessary is met (typically required further analysis)
- Utilized data collection forms (see next slides and handouts)
- Once forms completed, sent back to cost center for verification
- Business owners put on the hook for accuracy
- Identified cost centers that require more attention (e.g., sales)



Use Form

(handout)



Cost Center Name and Name:

Job Title

Follow-Up (Y/N):

Manager:

Supplemental Contacts:

Name & Phone #

Name & Phone #

Job Category:

Do you need access to PHI to perform your job function?

Do you have access to employee PHI ?

Job Functions:	Electronic System Access (PHI Only)	Sub-System Level **Refer to Security Grid	Condition/ Type of Access	Non Electronic Access (PHI Only)	Condition/Type of Access

Comments:

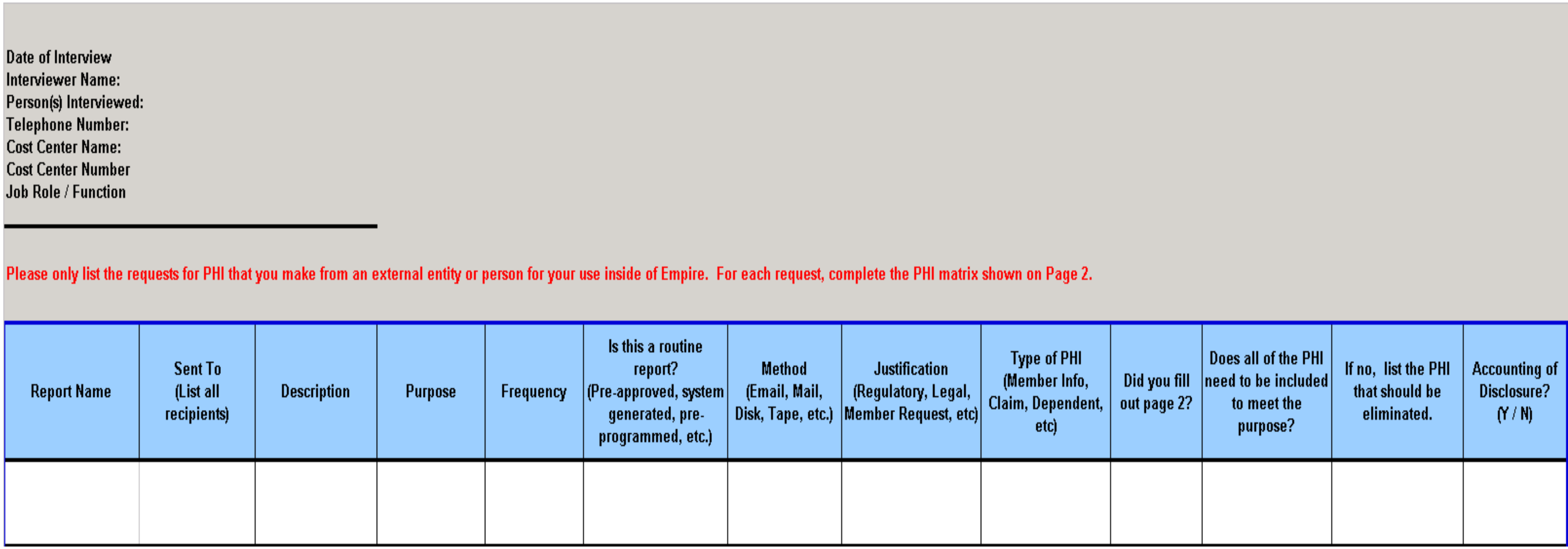
Findings:

Recommendations

Empire Privacy Access Control List

Category		Description
Read/view	R	Read the contents of a file, directory, or data
Add/change		
Create	C	Create a file in a directory, or add a new data
Delete	D	Remove a file, directory, or data element in a table.
Modify	M	Change the contents of an existing file or data
Execute	X	Run or launch program code.
Supervisor	S	Ability to grant system access control privileges to

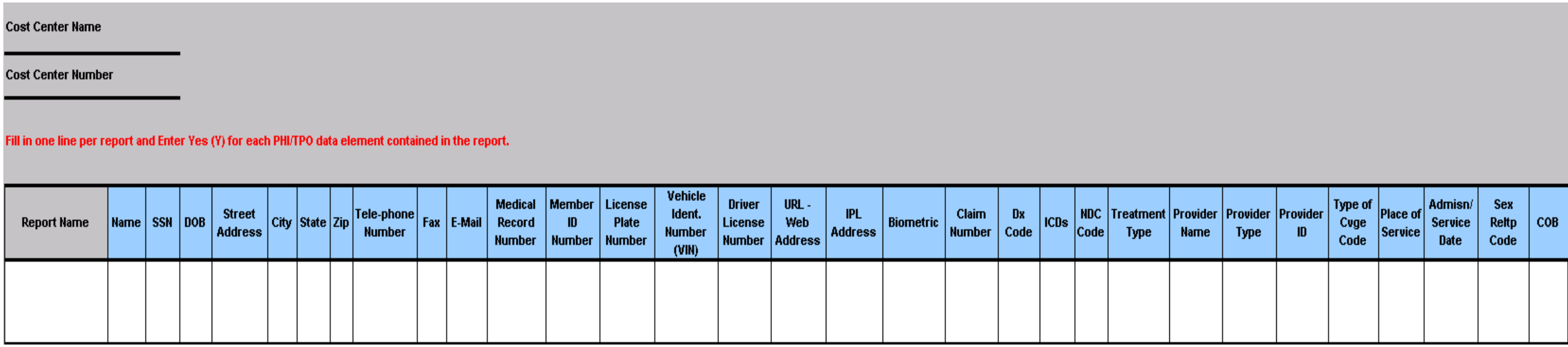
Disclosure Form -- Reports (handout)



Date of Interview
Interviewer Name:
Person(s) Interviewed:
Telephone Number:
Cost Center Name:
Cost Center Number
Job Role / Function

Please only list the requests for PHI that you make from an external entity or person for your use inside of Empire. For each request, complete the PHI matrix shown on Page 2.

Report Name	Sent To (List all recipients)	Description	Purpose	Frequency	Is this a routine report? (Pre-approved, system generated, pre-programmed, etc.)	Method (Email, Mail, Disk, Tape, etc.)	Justification (Regulatory, Legal, Member Request, etc)	Type of PHI (Member Info, Claim, Dependent, etc)	Did you fill out page 2?	Does all of the PHI need to be included to meet the purpose?	If no, list the PHI that should be eliminated.	Accounting of Disclosure? (Y / N)



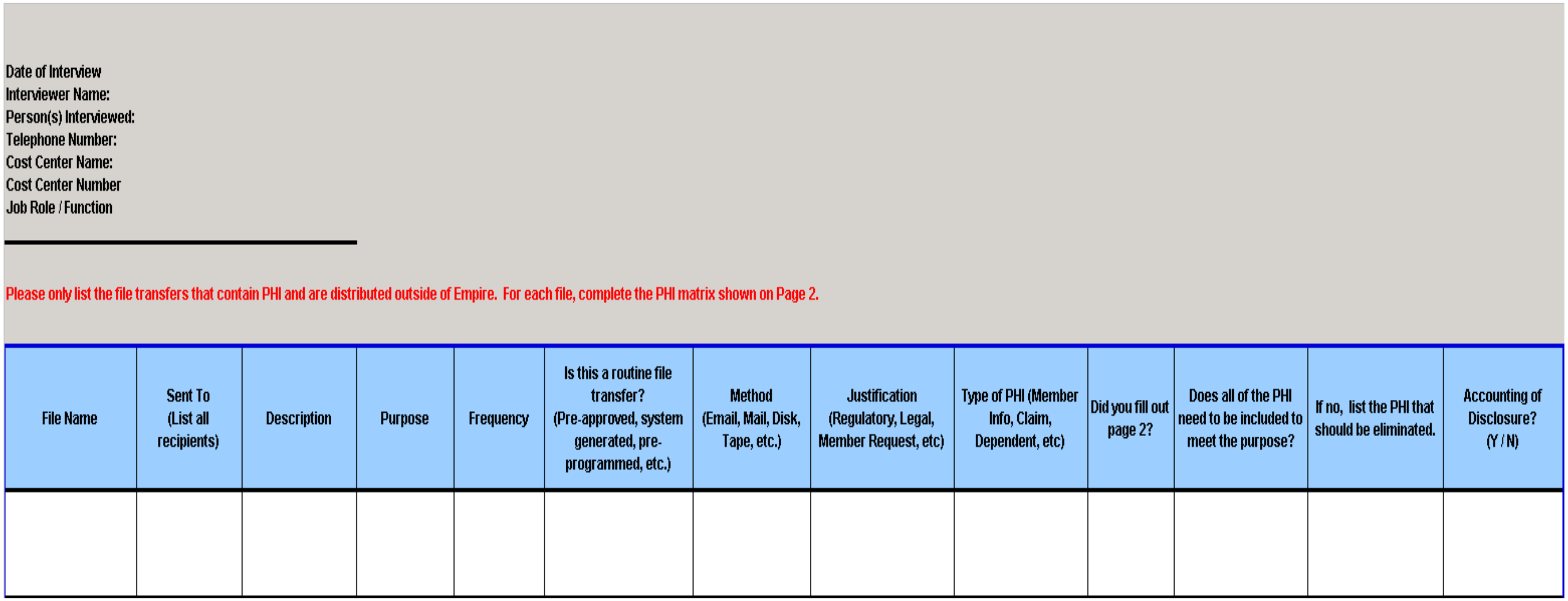
Cost Center Name

Cost Center Number

Fill in one line per report and Enter Yes (Y) for each PHI/TPO data element contained in the report.

Report Name	Name	SSN	DOB	Street Address	City	State	Zip	Tele-phone Number	Fax	E-Mail	Medical Record Number	Member ID Number	License Plate Number	Vehicle Ident. Number (VIN)	Driver License Number	URL - Web Address	IPL Address	Biometric	Claim Number	Dx Code	ICDs	NDC Code	Treatment Type	Provider Name	Provider Type	Provider ID	Type of Cvge Code	Place of Service	Admisn/ Service Date	Sex Reltp Code	COB

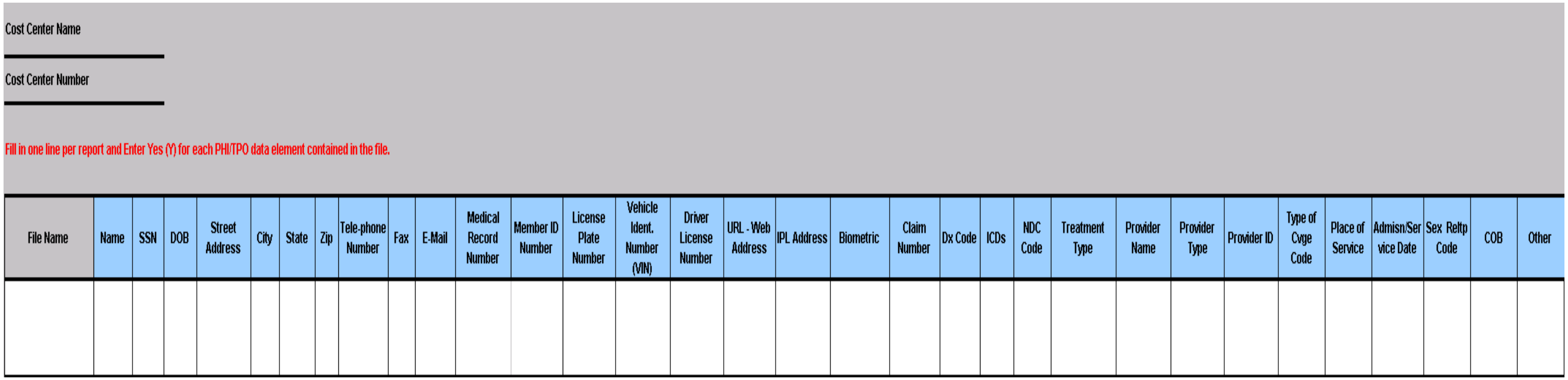
Disclosure Form – Files (handout)



Date of Interview
Interviewer Name:
Person(s) Interviewed:
Telephone Number:
Cost Center Name:
Cost Center Number
Job Role / Function

Please only list the file transfers that contain PHI and are distributed outside of Empire. For each file, complete the PHI matrix shown on Page 2.

File Name	Sent To (List all recipients)	Description	Purpose	Frequency	Is this a routine file transfer? (Pre-approved, system generated, pre-programmed, etc.)	Method (Email, Mail, Disk, Tape, etc.)	Justification (Regulatory, Legal, Member Request, etc)	Type of PHI (Member Info, Claim, Dependent, etc)	Did you fill out page 2?	Does all of the PHI need to be included to meet the purpose?	If no, list the PHI that should be eliminated.	Accounting of Disclosure? (Y / N)



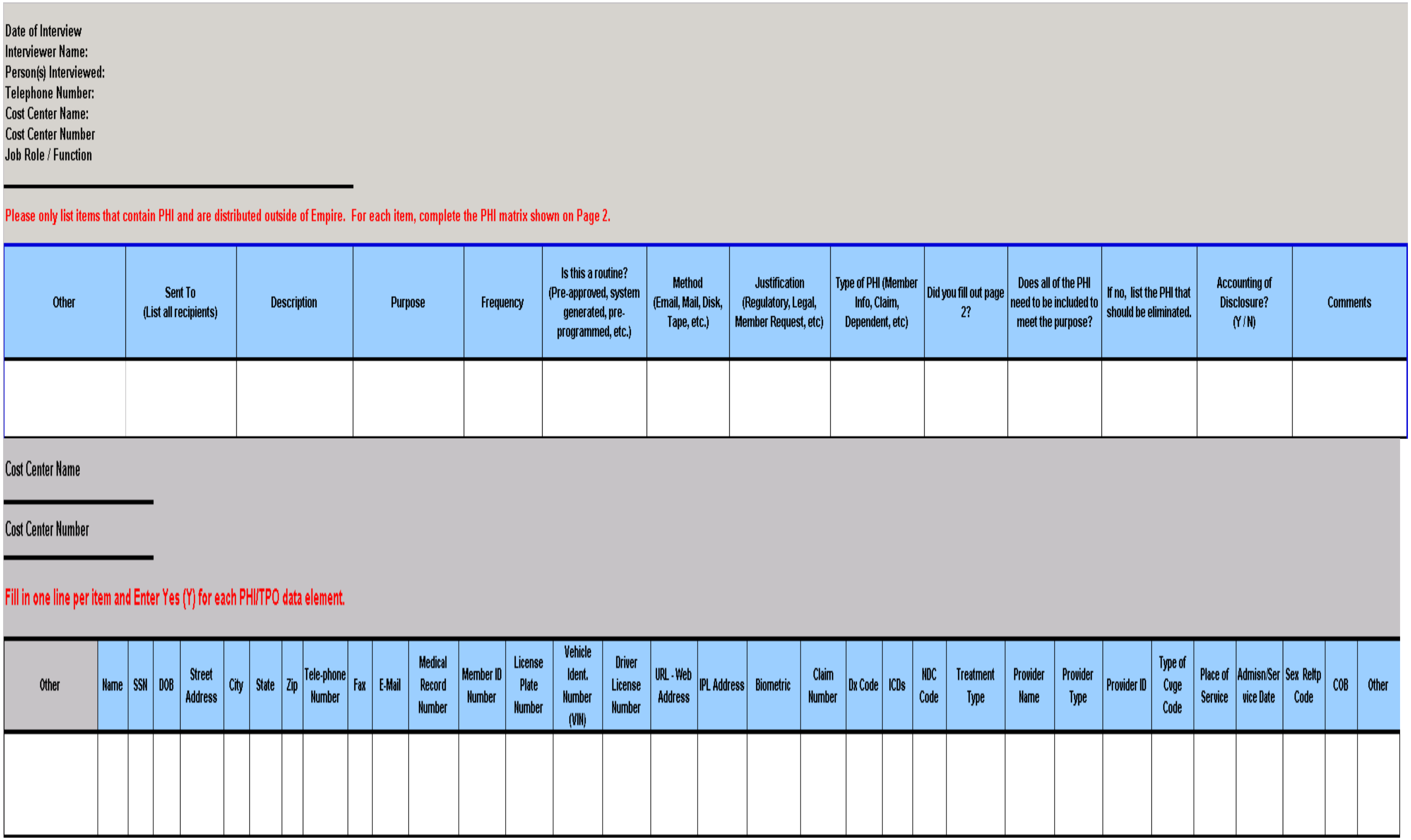
Cost Center Name

Cost Center Number

Fill in one line per report and Enter Yes (Y) for each PHI/TPO data element contained in the file.

File Name	Name	SSN	DOB	Street Address	City	State	Zip	Tele-phone Number	Fax	E-Mail	Medical Record Number	Member ID Number	License Plate Number	Vehicle Ident. Number (VIN)	Driver License Number	URL - Web Address	IPL Address	Biometric	Claim Number	Dx Code	ICDs	NDC Code	Treatment Type	Provider Name	Provider Type	Provider ID	Type of Cvge Code	Place of Service	Admisn/Ser vice Date	Sex Reltp Code	COB	Other

Disclosure Form -- “Other” (handout)



Date of Interview
Interviewer Name:
Person(s) Interviewed:
Telephone Number:
Cost Center Name:
Cost Center Number
Job Role / Function

Please only list items that contain PHI and are distributed outside of Empire. For each item, complete the PHI matrix shown on Page 2.

Other	Sent To (List all recipients)	Description	Purpose	Frequency	Is this a routine? (Pre-approved, system generated, pre-programmed, etc.)	Method (Email, Mail, Disk, Tape, etc.)	Justification (Regulatory, Legal, Member Request, etc)	Type of PHI (Member Info, Claim, Dependent, etc)	Did you fill out page 2?	Does all of the PHI need to be included to meet the purpose?	If no, list the PHI that should be eliminated.	Accounting of Disclosure? (Y / N)	Comments

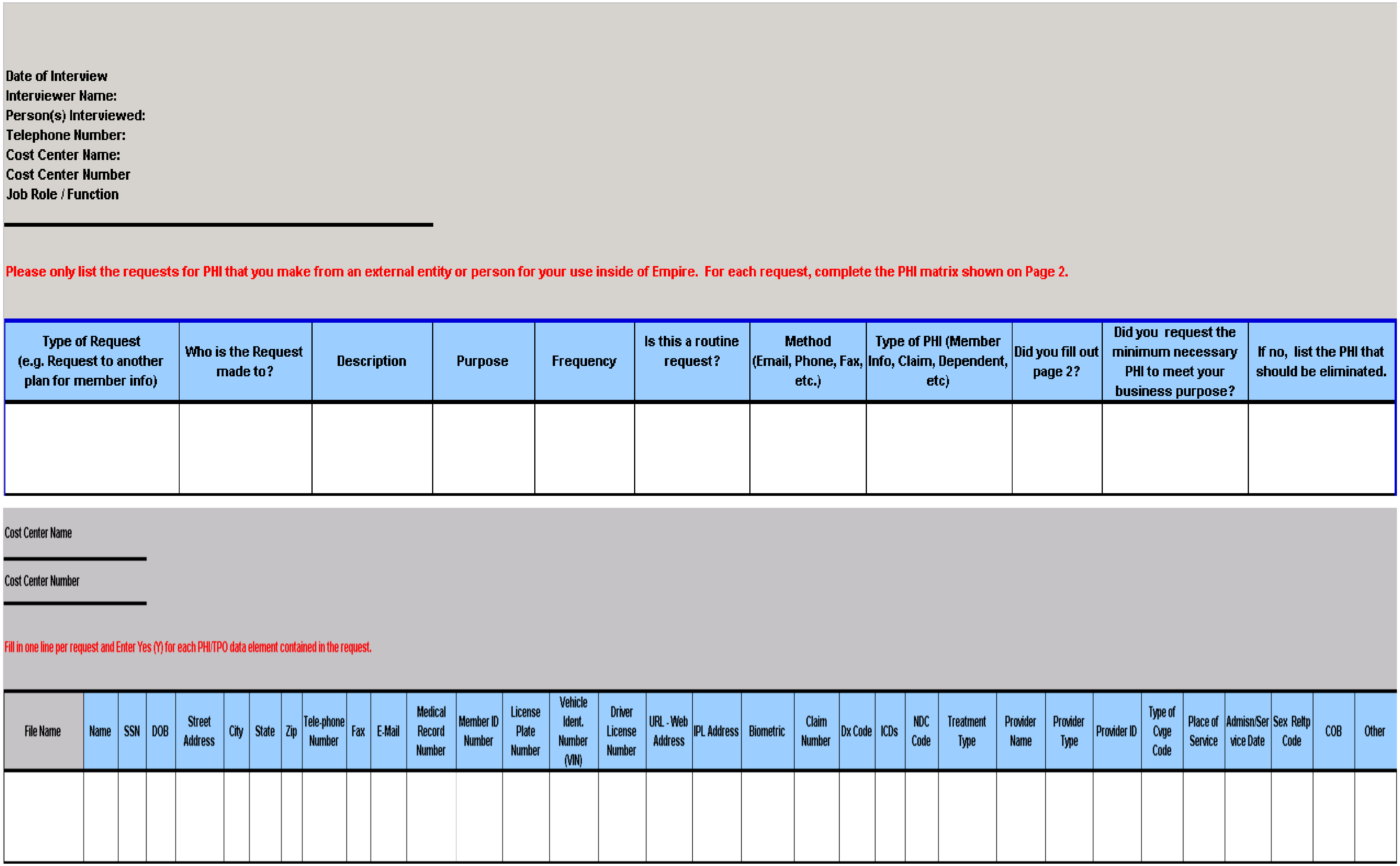
Cost Center Name

Cost Center Number

Fill in one line per item and Enter Yes (Y) for each PHI/TPO data element.

Other	Name	SSN	DOB	Street Address	City	State	Zip	Tele-phone Number	Fax	E-Mail	Medical Record Number	Member ID Number	License Plate Number	Vehicle Ident. Number (VIN)	Driver License Number	URL - Web Address	IPL Address	Biometric	Claim Number	Dx Code	ICDs	NDC Code	Treatment Type	Provider Name	Provider Type	Provider ID	Type of Cvge Code	Place of Service	Admisn/Service Date	Sex Reltp Code	COB	Other

Request of PHI Form (handout)



Date of Interview
Interviewer Name:
Person(s) Interviewed:
Telephone Number:
Cost Center Name:
Cost Center Number
Job Role / Function

Please only list the requests for PHI that you make from an external entity or person for your use inside of Empire. For each request, complete the PHI matrix shown on Page 2.

Type of Request (e.g. Request to another plan for member info)	Who is the Request made to?	Description	Purpose	Frequency	Is this a routine request?	Method (Email, Phone, Fax, etc.)	Type of PHI (Member Info, Claim, Dependent, etc)	Did you fill out page 2?	Did you request the minimum necessary PHI to meet your business purpose?	If no, list the PHI that should be eliminated.

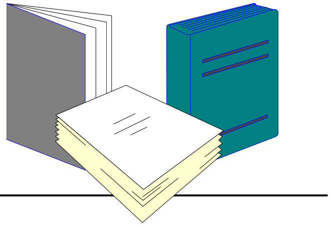
Cost Center Name

Cost Center Number

Fill in one line per request and Enter Yes (Y) for each PHI/TPO data element contained in the request.

File Name	Name	SSN	DOB	Street Address	City	State	Zip	Tele-phone Number	Fax	E-Mail	Medical Record Number	Member ID Number	License Plate Number	Vehicle Ident. Number (VIN)	Driver License Number	URL - Web Address	IPL Address	Biometric	Claim Number	Dx Code	ICDs	NDC Code	Treatment Type	Provider Name	Provider Type	Provider ID	Type of Cvge Code	Place of Service	Admisn/Ser vice Date	Sex Reltp Code	COB	Other

Minimum Necessary Policy



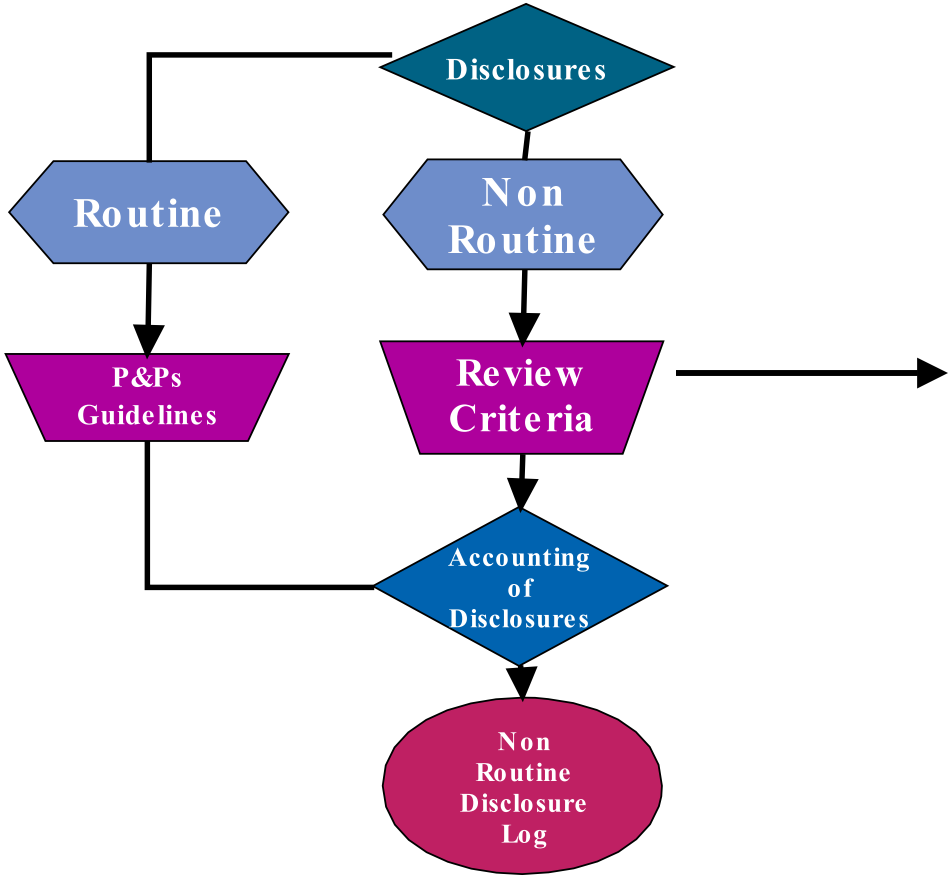
- "Empire BlueCross BlueShield will make reasonable efforts to limit its uses and disclosures of protected health information (PHI) and to limit its requests for PHI from another covered entity to the minimum necessary to accomplish the intended purpose of a use, disclosure, or request.
- Empire BlueCross BlueShield also will make reasonable efforts to limit its uses and disclosures of PHI to those members of its workforce and authorized third parties who need PHI to carry out their duties for Empire BlueCross BlueShield .

The corporate wide MN Policy incorporates all MN procedures, related security policies, standards and procedures by reference.

Minimum Necessary Standard Operating Procedures

- **Purpose**
  - Define manager and staff responsibilities and procedures
- **Manager**
  - Assign access for staff (link to security)
  - Review and document routine and non routine disclosures and requests
  - Develop “standard guidelines” for routine disclosures and requests
- **Staff**
  - Permitted PHI uses, disclosures, requests
  - Routine and non routine procedures
  - Responsibilities to report violations
  - Link to security
  - Sanctions
- **Other content**
  - Entire medical record justification
  - Business Associates
  - Relying on requests of other entities
  - Exceptions to minimum necessary

Individual Review Criteria – Deciding How Much to Disclose

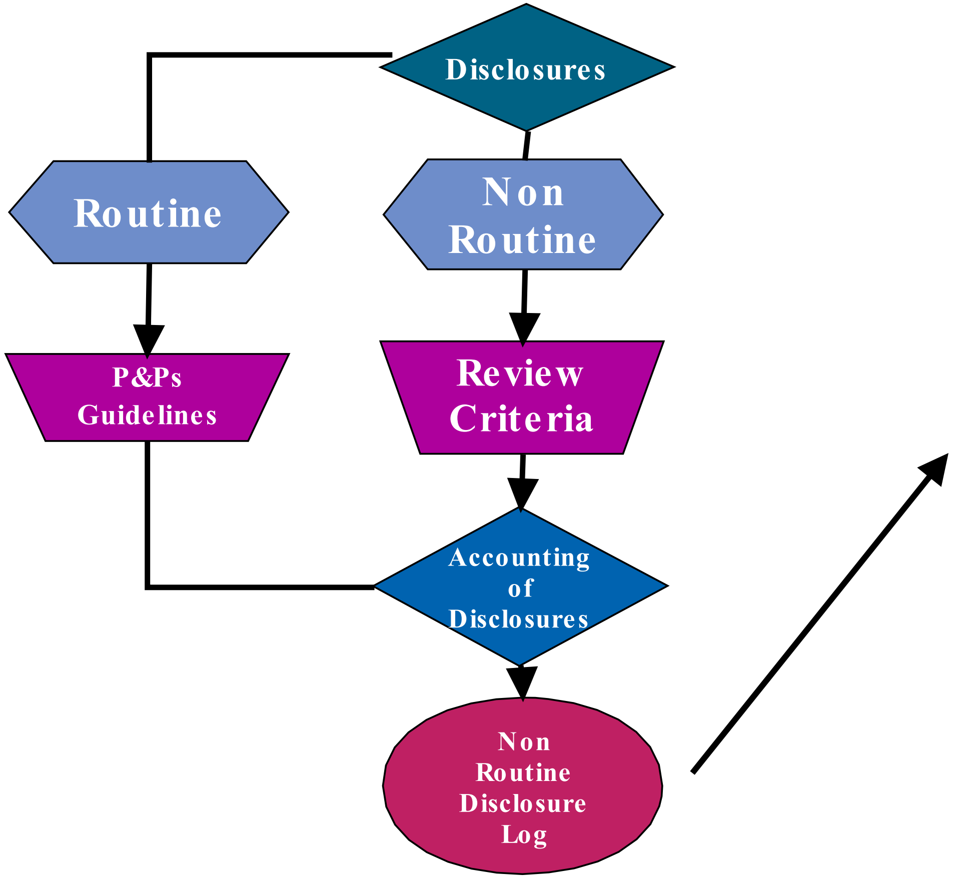


Balancing Factors

- ➢Who is the requestor
- ➢Purpose of request
- ➢PHI requested
- ➢Impact to individual (harm?)
- ➢Likelihood of re-disclosure
- ➢Other sources of this PHI
- ➢Can other PHI be removed
- ➢Involves other laws
- ➢Can requestor be relied upon to be minimum necessary
- ➢Adequacy of safeguards

(same process for requests)

Non Routine Disclosure and Request Log



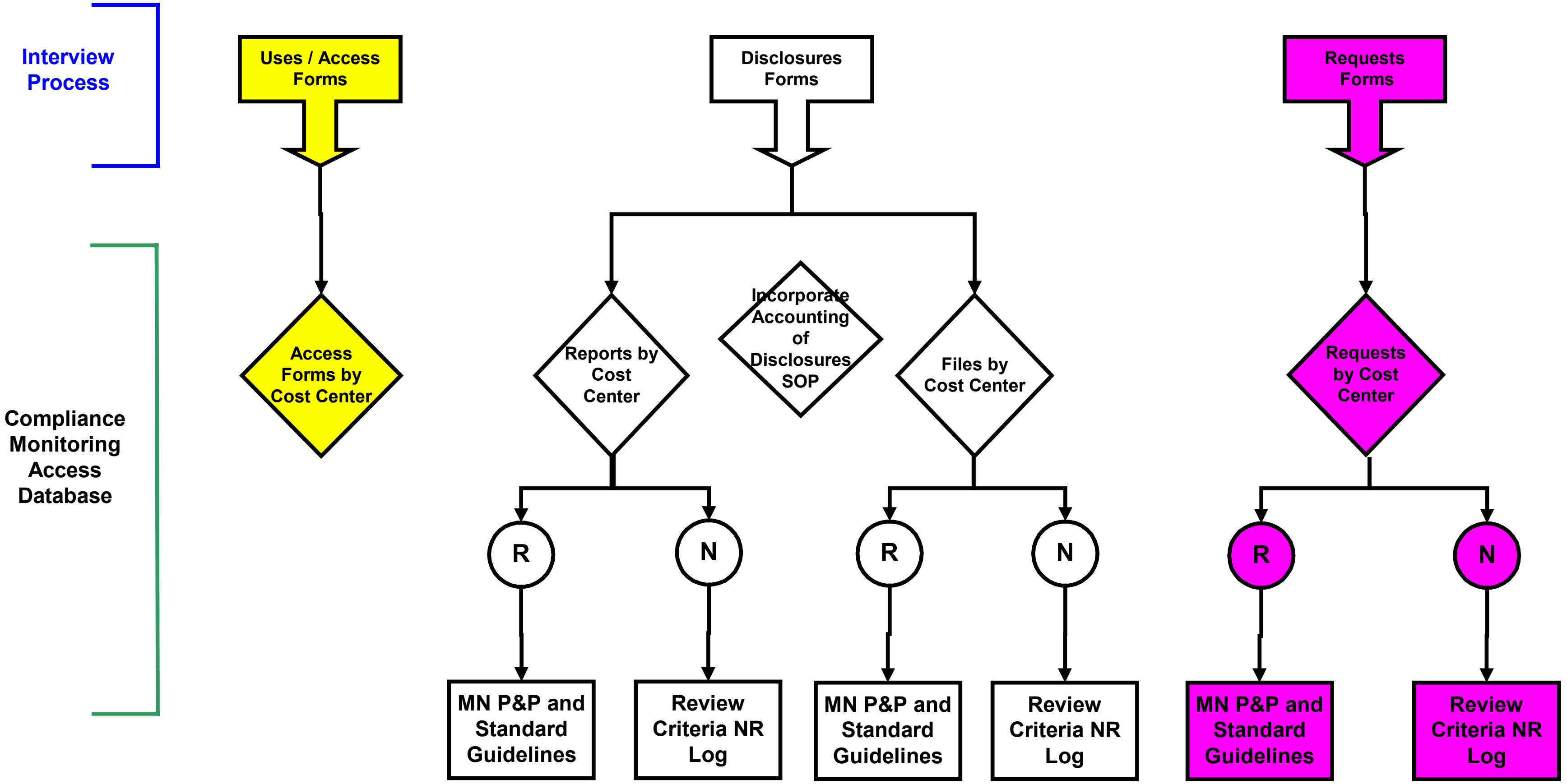
Log Content

- ➢Name of staff disclosing
- ➢Recipient of the data
- ➢Date disclosed
- ➢Type of data disclosed
- ➢Department manager approving disclosure

Log can be manual or automated in a central location

Incorporating Minimum Necessary into a Compliance Monitoring Process

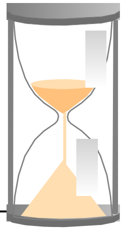
Compliance Monitoring Minimum Necessary Database



Access Database Capabilities

- Tool for monitoring compliance
- Provides snapshot of use, disclosures, requests
- Identifies and compiles disclosures and requests of PHI
- Ability to query on many variables
  - by cost center, purpose of disclosure, categories of PHI, reports/files that currently meet/don't meet MN, recipients of disclosures, accounting of disclosures, etc.
- Identifies in one place members of workforce that require access to PHI
- Tracks progress towards compliance (can establish baseline reports)
- Staff can quickly update forms
- Leads to the development of MN guidelines/manual per cost center
  -

Lessons Learned



- It takes time – it’s harder than you think
- Involves almost all departments of your organization
- Hold joint privacy and security work sessions (identify interdependencies)
- Education is key – there is a need for level setting on requirements
- Essential to identify where PHI is located in your organization
- Understand current and future system capabilities (e.g., level of access)
- Business decision whether to go to PHI data element level or some other category
- Don’t forget what your business associates have access to

Lessons Learned

- Make business owners accountable
- Remember share drives may contain PHI
- Don’t forget about HR (assist in job roles, functions, etc.)
- Think ahead – use tools for compliance monitoring purposes
- Don’t forget about the regulatory exceptions
- Define and document “routine” (may include ad hocs that happen weekly)
- Link in whether an accounting of disclosure is required
- Incorporate into training

“the lack of adequate security can increase the risk of violation of the privacy standards”

- HHS

Questions?