SESSION 2.3
Practical Initiatives in Complying With HIPAA and California's Health Care Privacy and Security Laws and Regulations

The Hospital / Health System Perspective

Ross Hallberg
Corporate Compliance Officer

John Muir / Mt. Diablo Health System

John Muir / Mt Diablo Health System

- Located in the San Francisco Bay Area - (corporate offices in Walnut Creek)

- A not-for-profit, multi-entity, integrated health system

- 12 entities include two acute care hospitals, a behavioral medicine and psychiatric hospital, a home health agency, ambulatory surgery centers, outreach Laboratory services, several outpatient service entities, and a foundation model entity that owns 71 physician practices in 19 locations, serving approximately 73,500 covered lives

- We also operate our county's only Trauma Center
  - 733 square miles and a population of 972,000

Health Insurance Portability and Accountability Act

- 7 different "Titles"
- Originally was a law protecting the health care coverage of employees when they change jobs
- **Administrative Simplification** (patient information) "tacked on" by Congress
- Congress didn't enact implementing legislation within its own deadline, so the Clinton administration issued the regulations we now call HIPAA

Parts of Administrative Simplification

- New Electronic Claims and Other Standard Transactions & Code Sets (TCS)
- Increased Protection of the Privacy and Confidentiality of Patients' Health and Medical Information (Privacy)
- New Standards for Security of Patient Health and Medical Information (Security)
- 4 new Standard Identifiers

Administrative Simplification - Who's a Covered Entity?

Health Plans/Payers.

- "Any individual or group health plan that provides or pays the costs of medical care."

Health Care Clearinghouses.

- "Entities that process healthcare information into standard data elements for electronic or other transmission, such as billing services, management information services and community health information systems."

Health Care Providers.

- "Any person or entity that furnishes or bills and is paid for health care services in the ordinary course of business. However, only providers who transmit health information, specified in any of the standard transactions, electronically, are covered entity providers."

HIPAA Transaction & Codes Sets

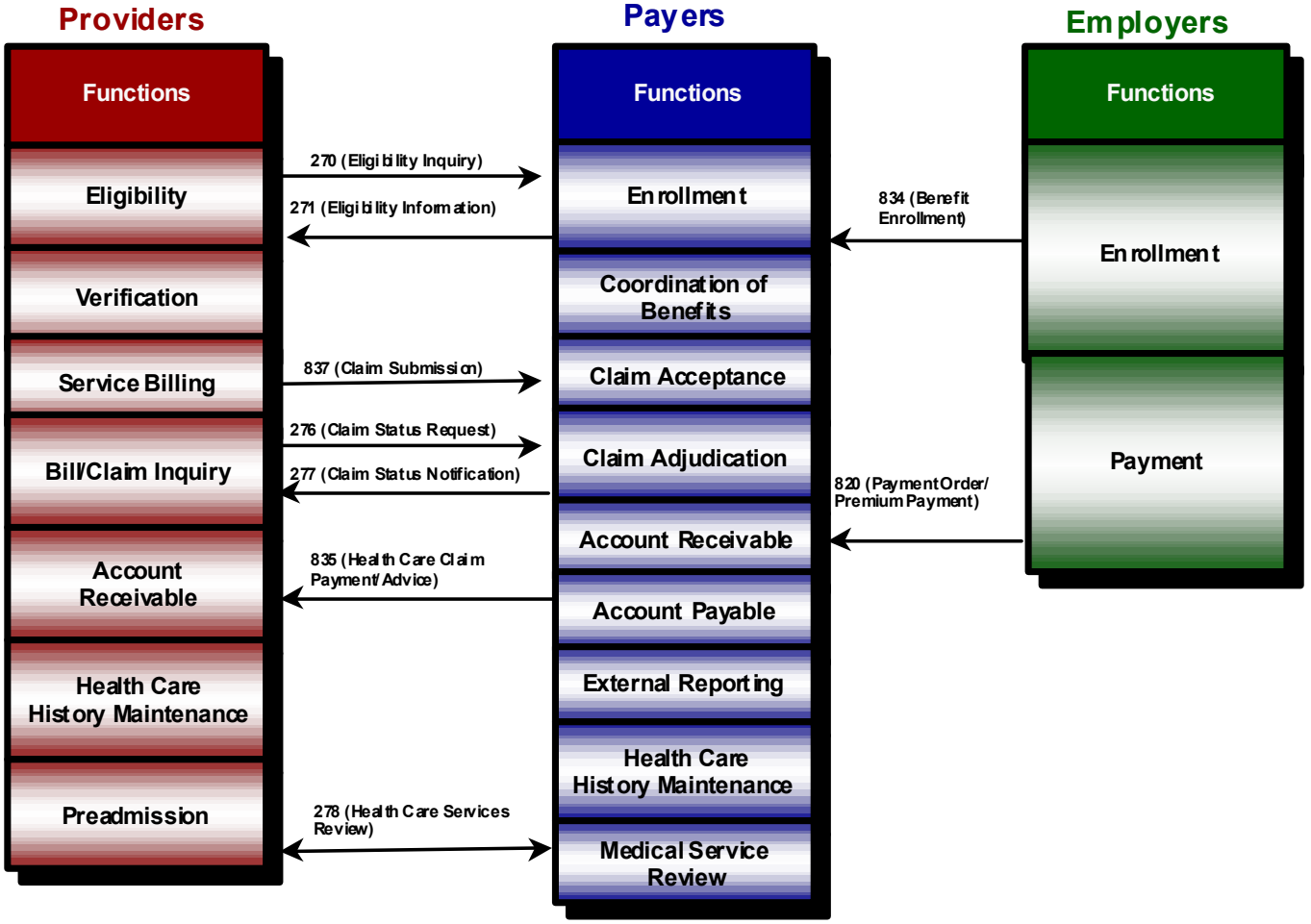
Transactions and Code Sets (TCS) regulations establish:

- Unique national standards for the electronic exchange of the following types of transactions:
  - Health Claims or Equivalent for Encounters
  - Enrollment/Disenrollment in a Plan
  - Eligibility Verification for a Plan
  - Health Care Claim Payment & Remittance Advice
  - Health Plan Premium Payments
  - Health Claim Status
  - Referral Certification & Authorization
- Specific code sets to be used in the electronic transactions.
- Requirements concerning the use of these standards by health plans, health care clearinghouses, and most health care providers.

The compliance deadline for HIPAA TCS is October 16, 2003.

EDI - Standard Electronic Transactions

HIPAA specifies standard electronic transaction formats and code sets for specific interactions among providers, health plans / payers, and employers



Required Code Sets

These code sets have been established as the standard medical data code sets for use in the standard transactions:

(A) **ICD-9- CM:** international classification of diseases, 9th edition, clinical modification**,** volumes 1 and 2 (including The official ICD-9-CM guidelines for coding and reporting), as maintained and distributed by DHHS.

(B) **ICD-9- CM volume 3 procedures:** international classification of diseases, 9th edition, clinical modification, (including The official ICD-9-CM guidelines for coding and reporting), as maintained and distributed by DHHS.

(C) **national drug codes (NDC):** as maintained and distributed by DHHS, in collaboration with drug manufacturers. Unclear if physician practices must use these code or existing codes.

(D) **code on dental procedures and nomenclature:** as maintained and distributed by the American Dental Association, for dental services.

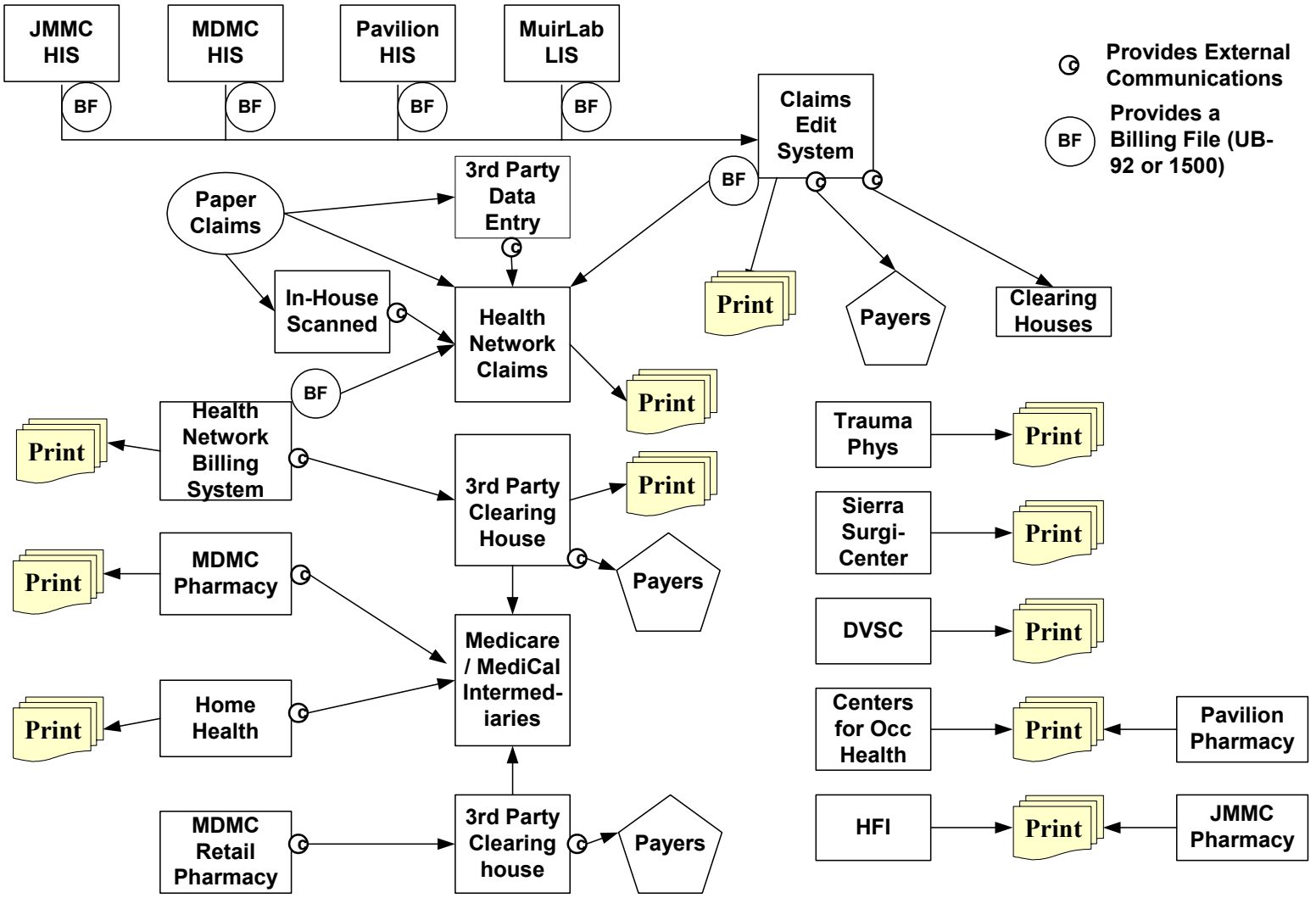
(E) **CPT-4:** current procedural terminology, fourth edition, as maintained and distributed by the American Medical Association, for physician services and other health care services.

(F) **HCPCS:** The health care financing administration common procedure coding system, as maintained and distributed by DHHS, for all other substances, equipment, supplies, or other items used in health care services.

Transaction Systems Inventory & Audit

- Here's what we found:
  - 15 Applications that generate claims, but no other transactions. No central management
  - Of the 15, 13 bill Medicare in some form (UB, 1500, NCPDP)
  - Of the 15, 10 are performing some level of electronic transmission of claims to Medicare, other payers and/or clearinghouses (and 5 are printing paper claims)
  - 1 additional application that receives and adjudicates claims from other providers -- accepts both manual and electronic claims. Creates paper Remittance Advices.
  - That is, we are both a payer and a provider.

Current Claims Environment



Our Understanding of the HIPAA Vision

- The regulations specify data content and format requirements for 9, high volume, mostly (currently) manual transactions

- The vision is to enable healthcare entities to replace expensive, labor intensive, time consuming, inaccurate manual processes (phone calls, faxing, email, letters, paper documents, etc.) with a standardized set of fully automated processes

- If automation can replace manual processes in these and other transactions, millions of dollars could be saved by most payers and providers through elimination of labor and work process redesign.

Achieving the Vision

To achieve the vision, 5 components are necessary, and each involves a significant effort:

1. **Standard data content.** The regulations specify what elements of patient information are to be communicated, and what the meaning of each data element is.
2. **Standard data formats.** The sequence of the data elements must always be the same, or each organization will not know which data element is which. The regulations specify the formats for the transactions.
3. **Communication of the transactions.** It won't help to be able to gather all the required data elements and put them in the proper electronic sequence, if there isn't some way to send the transactions back and forth between providers, payers, and others involved. Appropriate communications technologies are required. The regulations don't specify the communications protocols. It's up to each pair of senders and receivers (trading partners) to agree on these protocols.

Achieving the Vision

- **5 Components are Required (Continued):**

4. **New software applications**. Even if the standard transactions can be communicated properly, the goal of replacing expensive, manual processes with automated processes cannot happen unless vendors add new application programs and functions. Today's software will not do the job. We are using it to support all the current manual processes! New applications must be developed to properly utilize the electronic transactions and provide the basis and means for us to replace the current manual processes.
5. **New Work Processes**. Even if the vendors create the necessary applications to fully utilize the electronic transactions, the cost reductions and other benefits will not be achieved unless we redesign all the work processes associated with the transactions and eliminate the labor and manual functions currently in place.

Like Most of You, We are Heavily Vendor Dependent

What if they don't come through on some, most, or all of the first 4 components?:

1. **Data Content**
2. **Standard Formats**
3. **Communications**
4. **New Applications**

Then We'll Have To Do It!

Capabilities required to manage communications:

- Checking, editing, and validating the transactions before they are sent out, handling error conditions with the vendor application system, etc.
- Routing compliant transactions outbound to payers or clearinghouses using a variety of protocols and infrastructures (dial-up, Intranet, etc.) using both batch and real-time technologies, handling error conditions, flow controls, etc.
- Monitoring for and receiving inbound transactions from payers and clearinghouses using both batch and real time technologies.
- Routing inbound transactions to the proper applications system in a way and format that the system can accept them.

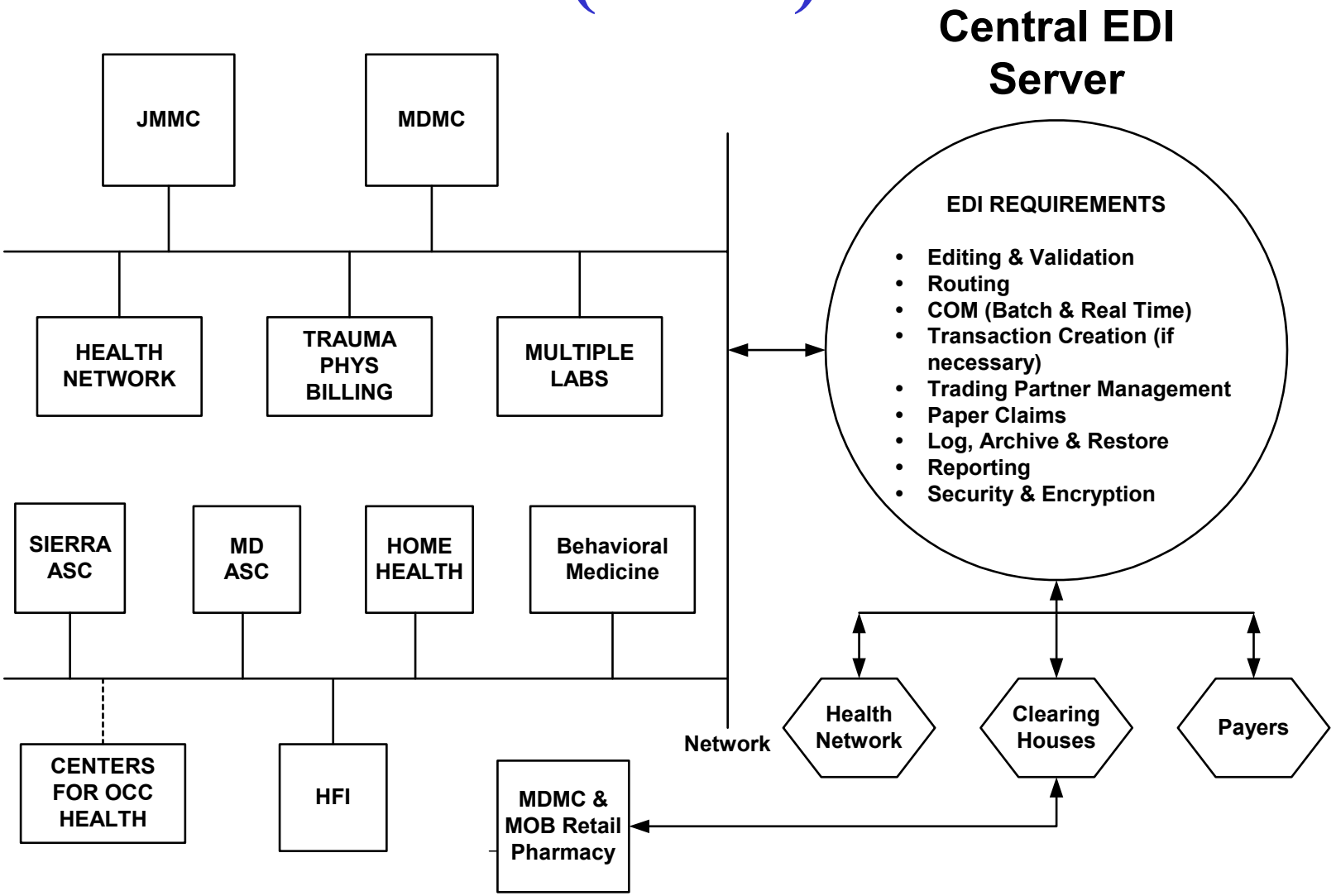
Then We'll Have To Do It! - cont'd

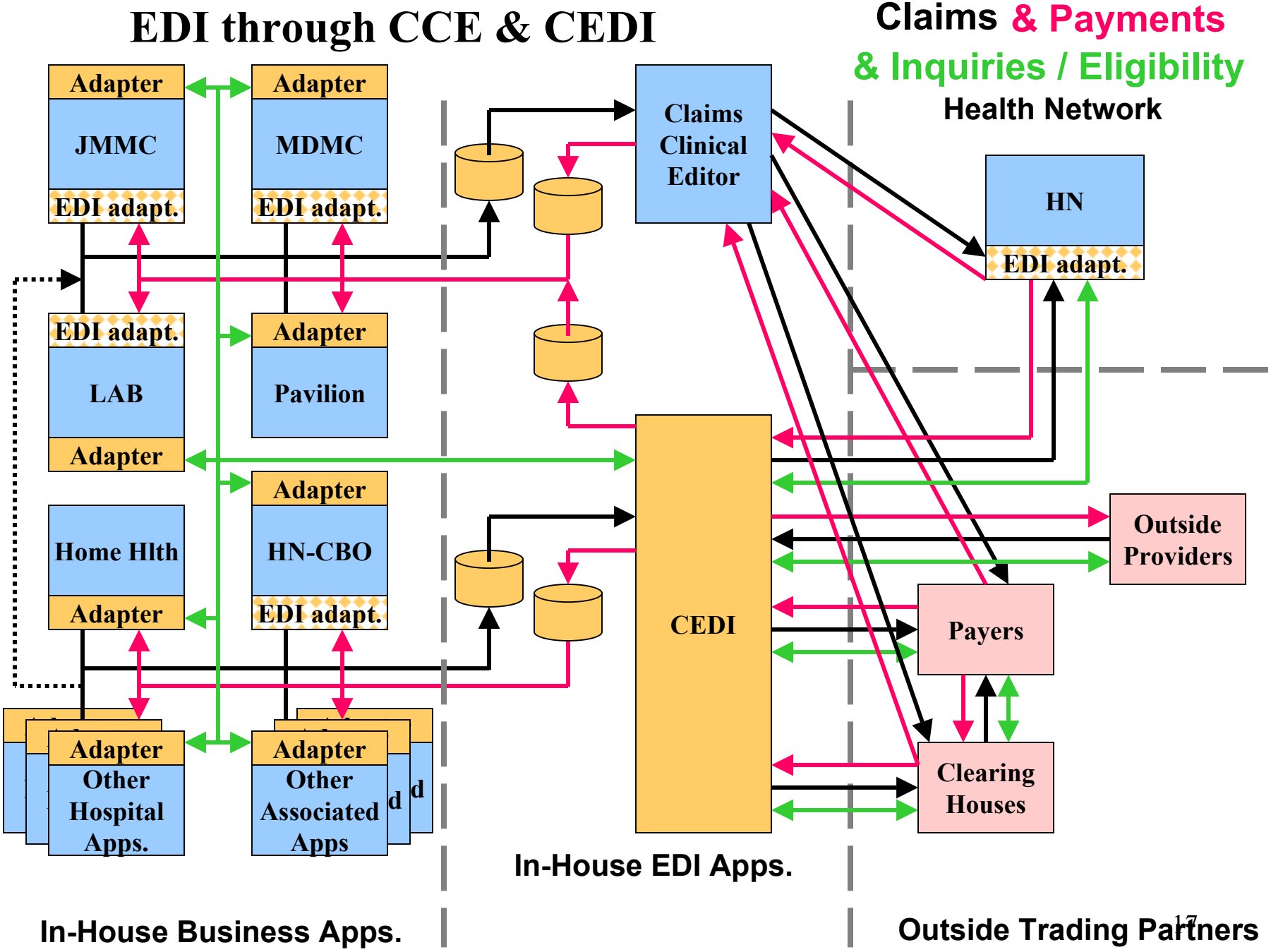
- Managing trading partner (payer and clearinghouse) communication details that are not specified in the transaction standards (e.g. whether or not dashes are put in the SSAN, the delimiters used within and between records, the structure and sequence of the records in the transmission, etc.
- Logging Records of the transactions, error handling, archiving, restoring from failures, etc.
- Reporting
- Security and Encryption

Additional requirements if vendors won't structure valid transactions:

- Multiple capabilities to extract the required data content from a vendor's system and/or gather data outside a vendor's system.
- Converting extracted data elements, however they might be obtained, into the required transaction formats.

The JMMDHS Central EDI Service (CEDI)




EDI through CCE & CEDI
Claims & Payments
& Inquiries / Eligibility
Health Network
Adapter
JMMC
EDI adapt.
Adapter
MDMC
EDI adapt.
Claims
Clinical
Editor
HN
EDI adapt.
EDI adapt.
LAB
Adapter
Adapter
Pavilion
Home Hlth
Adapter
Adapter
HN-CBO
EDI adapt.
CEDI
Outside
Providers
Payers
Clearing
Houses
Adapter
Other
Hospital
Apps.
Adapter
Other
Associated
Apps
In-House EDI Apps.
In-House Business Apps.
Outside Trading Partners

CEDI Project

- CEDI project was established to research and acquire software, hardware, and staffing (1 FTE) for development of adapters and background agents
- CEDI application will automate all steps after production of the raw claim in the business applications
- CEDI project will also be called upon to create “adapters” which will extract data (or can be used in conjunction with the business applications to gather additional data)
- CEDI project must have the capacity to accommodate additional transactions and to take up the “slack” in the other business systems where they have not been appropriately tooled.

HIPAA Privacy Regulations -- What Medical Information is Covered?

- "Medical Information" (CA regulations) and Protected Health Information (HIPAA) have essentially the same meaning.

- Protected Health Information (**PHI**) is patient information that is created, maintained, used, disclosed, or transmitted in any form – electronic, written or oral.

  - To be PHI under the regulations, the information must:

    (1) relate to a person's past, present, or future physical or mental health condition, the provision of health care, or the payment of health care.

    (2) identify, or be usable to identify, the person who is the subject of the information.

HIPAA Privacy Regulation

Major provisions of the privacy regulation that will require effort on the part Covered Entities:

A. Uses and Disclosures of PHI – General Rule.
   1. Minimum Necessary.
   2. Business Associates (BA).
   3. Personal Representatives.

B. Uses and Disclosures of PHI– Specific Requirements.
   1. Notice of Privacy Practices.
   2. Authorizations.
   3. Disclosures without Authorizations.
   4. Uses and Disclosures Requiring an Opportunity to Object.

C. Other Use and Disclosure Requirements.
   1. Marketing and Fundraising .
   2. Data De-Identification.

HIPAA Privacy Regulation

Major provisions of the privacy regulation that will require effort on the part Covered Entities:

D. Patient Rights Under the Regulations.
   1. Access to Health Information.
   2. Amendment of Health Information.
   3. Right to Request Privacy Restrictions.
   4. Accounting of Disclosures.

E. Administrative Requirements.
   1. Privacy Safeguards.
   2. Training

F. Federal vs. State Law.
   1. The more restrictive law takes precedence.
   2. In California, the main regulation is the Confidentiality of Medical Information Act.

Privacy Technology Issues

Projects implemented and in use

- Intranet being used to organize and make available, regulations, presentations, and resources. Also used to facilitate policy and procedure development.
- Business Associate database developed to facilitate inventory, evaluation, and manage the process of Agreement execution / completion.
- Privacy Safeguards (eg: access, security)

Planned but not in use yet

- Web enabled training and education system

Open technology issues

- Notice of Privacy Practices acknowledgement tracking
- Patient Authorization strorage and retrieval
- Requests for PHI Restrictions
- Tracking of specific PHI disclosures for the Accounting of Disclosures requirements
- Status of topics when patient has the right to agree or object to specific PHI disclosures.
- Privacy Safeguards

Vendor Issues

Security Standards

- Covers all data maintained in electronic state.
- Data must be protected in four ways,
  1. **Administrative Procedures** (e.g., policy and procedures, employee training).
  2. **Physical Safeguards** (e.g, assigned security responsibility, Media controls, physical access controls, policy guidelines on workstation use, secure workstation locations, training).
  3. **Technical Security Services** (e.g., access controls, audit controls, authorization controls, data authentication, entity authentication).
  4. **Technical Security Mechanisms** (e.g., communications network controls, electronic signature)

HIPAA SECURITY REQUIREMENTS

A. Administrative Procedures

.Certification
.Contingency Plan
.Formal access control protocols
.Personnel Security
.Security Incident process
.Termination Procedures
.Chain of Trust Partner Agreement
.Formal mechanism for record processing
.Internal Audit
.Security Configuration Management
.Security Management process
.Training

B. Physical Safeguards

.Assigned security responsibility
.Physical access controls
.Secure workstation locations
.Media controls
.Policy/guideline on workstation use
.Security awareness training

C.Technical Security Services

. Access Control
. Authorization Control
. Entity Authentication
Audit Controls
. Data Authentication

D. Technical Security Mechanisms

. Communications/network controls

E. Electronic Signature (Optional)

C. Technical security services

Relates to services needed to guard data integrity, confidentiality, and availability - these include the processes that are put in place to protect and to control and monitor information access

1. Access Controls

Def: Required to restrict access to resources and only allow access to privileged. The following implementation feature must be implemented: Procedure for emergency access. In addition, at least one of the following three implementation features must be implemented: Context-based access, Role-based access, User-based access.

Implment Acty: Context-based access, Encryption, Procedure for emergency access' Role-based access, User-based access.

2. Audit controls

Def: Required to place an audit control mechanism to record and examine system activity. Audits would involve setting various rules and then reviewing them for violation attempts (e.g. time of day access).

Implement Acty: Audit control mechanism

3. Authorization controls

Def: Mechanism to obtain consent for the use and disclosure of health information to ensure that health information is used only by properly authorized individuals through either role-based or user based access.

Implment Acty: Role-based access. User-based access

C. Technical security services (continued)

Relates to services needed to guard data integrity, confidentiality, and availability - these include the processes that are put in place to protect and to control and monitor information access

4. Data Authentication

Def: Mechanism to ensure data entered is accurate. Required to provide corroborate that data has not been altered or destroyed in an unauthorized manner.

Implment Acty: Check digits, Double keying, Digital signatures

5. Entity authentication

Def: Required to corroborate that an entity is who it claims to be. The following implementation features must be implemented: Automatic logoff, Unique user identification. In addition, at least one of the other listed implementation features must be implemented.

Implment Acty: Automatic logoff, Biometric access, Password, PIN, Telephone callback, Token.

Information Security Objectives

Provide processes and methodologies to develop and sustain effective information security programs that support our business environments and the Privacy requirements

- Specify a standards-based information management approach for a set of role-based security solutions
- Reduce the complexity of establishing and maintaining security and reduce costs and business risk levels

Ensuring patient data confidentiality and privacy

- Prevent illegal access and confidential patient information disclosure from employees, contractors, vendors, and business associates.

Implementing State and Federal-Compliant Security Policy

- Simplify the process of deploying a written security policy into a production environment

Protecting Corporate Assets from Unauthorized Users

- Deliver the highest level of protection to our network and system resources with technology, which examines all aspects of network traffic – including the application level.

Planning Steps

Assessing the organization's readiness and risks

Security and Planning Management

- Plan for compliance with industry, State and Federal security standards
- Policy, procedures, and other documentation for compliance
- Contingency and disaster recovery planning

Defining and developing security measures

- Capitalize on best-practice information integration, security development and end-user education
- Developing baseline policies and security controls
- Develop security training, education and awareness program

In-depth Operations and Business Analysis

- Security Risk Analysis/ Risk Management Approach
- Business and Operations Business Continuity Disaster Recovery Planning
- End-to-End Security Architecture Definition

Develop documentation that recommends a solution, and provides a high-level project plan.

Path Forward - 2002/2003

- Perform an enterprise-wide business and operations process review and information workflow analysis
- Conduct gap analysis of information security policies and procedures to determine regulatory compliance posture - establish the baseline for comparison.
- Create a blueprint for strategically aligning the Health System to a regulatory and business compliant information infrastructure, and for monitoring compliance and detecting security breaches.
- Develop a strategic business plan that includes a risk assessment, potential solutions, a framework for risk management, and a mechanism for prioritizing those solutions.
- Breakdown the technical activities and processes necessary to meet the business and compliance objectives.
- Identify the types of resources (personnel, hardware, software, tools) needed to perform the technical activities.

An Example

Objective:

- Provide physicians with anytime, anywhere, PDA-type access to patient clinical information while meeting the HIPAA Security standards; and not impacting HIPAA Privacy compliance with regard to the use and disclosure of the PHI