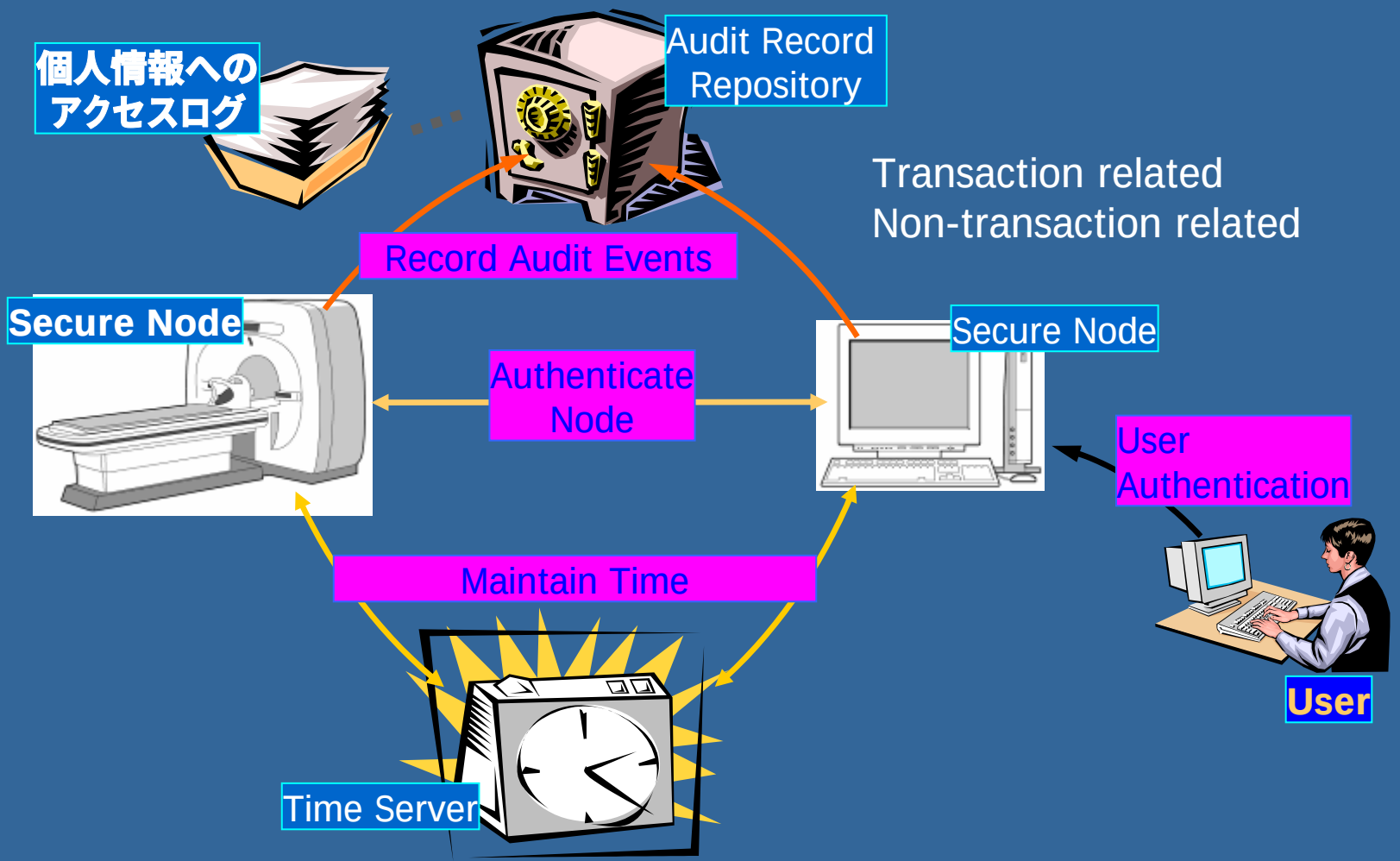
監査証跡とノード認証・時刻の整合性
放射線部門オプション

Audit Trail and Node Authentication
Radiology Option
Consistent Time

ATNA・CT

ATNA＋CT の仕組み


個人情報への
アクセスログ
Audit Record
Repository
Transaction related
Non-transaction related
Record Audit Events
Secure Node
Authenticate
Node
Secure Node
User
Authentication
Maintain Time
User
Time Server

監査証跡とノード認証 (ATNA) + 放射線部門拡張
概要・スコープ

- 医療施設における安全な個人情報保護環境の一部として使用される個々のシステムにおける基本的なセキュリティ機能を定める。
  - ホスト単位の認証機能を提供し、EUAやXUAによるユーザ認証と関連して使用される
  - セキュリティや患者情報保護に関連した作業をモニタするための監査証跡機能を提供する

ATNAの目的

- 患者個人情報の保護とシステムの安全性を守る:
  - 倫理的および法的規制に適合する
- 医療施設全体での管理に便利:
  - 統一化され均質な監査システム
  - マルチベンダでの共通の対策により施設のポリシや手順の制定が単純になる
  - 共通の対策により管理がシンプルになる
- コードの再利用により開発および管理のコストが削減できる:
  - 一回の開発で複数のアクタに適用出るようになる
  - 異なったセキュリティポリシや規制の環境でも、一つの開発成果で対応できる

ATNA　セキュリティに関する要求

- **理由：臨床での使用とプライバシ**
  - 医療従事者は患者の診療情報にアクセスしなくてはならないが、その情報を他の者に開示してはならない
  - 許可されない者が業務の邪魔をしたり、データを変更したりできないようにすべきである
- **運用とセキュリティ機構により、下記を保証する：**
  - **機密性** (Confidentiality)
  - **完全性** (Integrity)
  - **可用性** (Availability)
  - **信頼性・確実性** (Authenticity)

ATNA ノード認証

- X.509 証明書をノードの識別と鍵として使う
- TCP/IP Transport Layer Security Protocol (TLS) をノード認証と, オプションの暗号化に使う
- アソシエーションの確立にセキュア・ハンドシェイク・プロトコルを使用する:
  - 暗号化プロトコルの識別
  - セッション鍵の交換
- アクタは許可されたノードの証明書リストを作れなくてはならない.
- ATNA は、現時点では、HTTP, DICOM, and HL7に対するメカニズムを指定する

ATNA 監査システム

- 法的な利用よりも監視の目的で設計されている。
- 2種類の監査メッセージ形式
  - 放射線IHE用暫定形式：放射線部門用の下位互換
  - IETF/DICOM/HL7/ASTM 形式、将来拡張可能
    - DICOM Supplement 95
    - IETF Draft for Common Audit Message
    - ASTM E.214
    - HL7 Audit Informative documents
- 両形式とも XML メッセージで、XML規格の拡張機能により、拡張が許されている。

ATNA　監査イベントの記録

- 監査記録の通信には、Reliable Syslog (RFC 3195) の使用が推奨されるが、BSD Syslog (RFC 3164) も放射線ＩＨＥのBasic Securityとの互換性のために使用しても良い。
- 監査証跡のイベントと内容はAudit trail events and content based on IETF, DICOM, HL7, 及び ASTM の規格に準拠する。また、放射線ＩＨＥの Basic Security の監査イベント形式も互換性のために許される。

セキュアノードになるためには

- ノードとなるシステム全体がセキュアでなくてはならず、部分的なアクタだけの対応では駄目
- ノードとなるシステム全体において、識別、認証、許可におけるユーザに対する適切なアクセス制御が必須である
- 診療情報を扱う全ての通信は、認証され、傍受を防がなくてはならない。
- 全ての保健医療情報に関する動作について監査証跡を生成しなくてはならず、IHEのアクタとしてのものだけでは駄目

セキュアノードになるためには

- 監査機能を付加するだけでなく、
  十分な効果を得るために以下を考慮すべき：
  - どのイベントについて監査すべきかを決めること
  - 実装する全てのアプリケーションにおいて、監査されるべきイベントを検出し監査メッセージを生成すること
  - 全ての通信経路が保護されていることを保証すること
  - 全てのローカルな資源は、ローカルなセキュリティ機構により守られていること
  - 下記の技術の組合せを確立する：
    - 時刻の整合性 (CT) プロファイルによる時刻の同期
    - 証明書の管理
    - ネットワーク構成

時刻の整合性 (CT)

- Network Time Protocol (NTP) version 3 (RFC 1305) を時刻の同期に用いる
- アクタは手動での調整をサポートすること
- 要求精度: 1 秒
- オプションとして Secure NTP を使用できる
- ATNA, EUA, XUAをサポートする場合はCTが必須


複数検査の一括処理
Presentation of Grouped Procedure
PGP

放射線検査の課題

- マルチスライスCTや高速MRIは、大量な画像を素早く生成する
  - ３０００枚以上の画像
  - 検査の一部が必要な場合、すべてを読み出すことは必要ない
- 複数のオーダが一つの撮影として実施される
- 検査全体は、一人の読影医だけでは読影されない
- 主治医は、検査全体には興味は無い
- それぞれの要求手続きの進歩が把握できない

PGPのユースケース

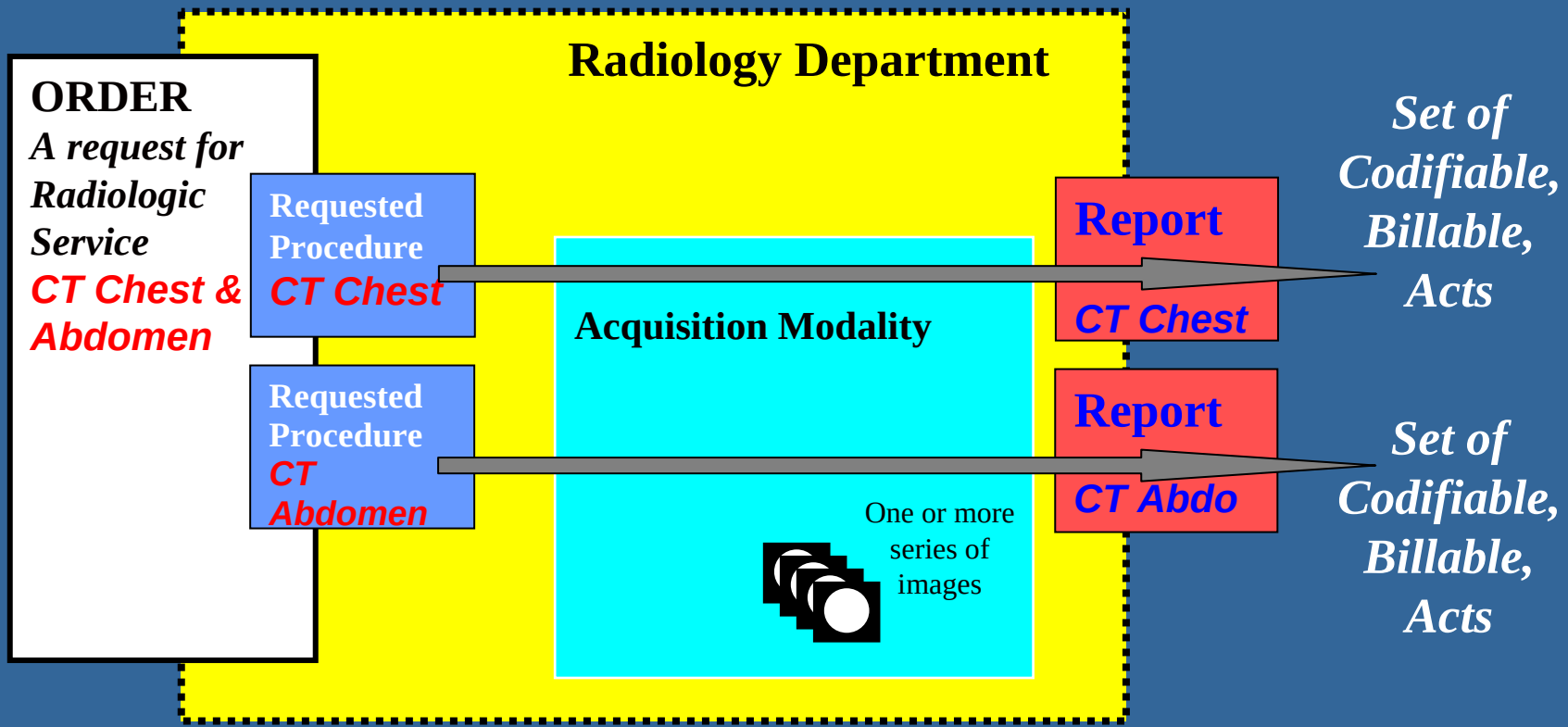
- CTによる胸部･腹部･骨盤の撮影
- 神経放射線：CTによる頸部と胸部の撮影
- MRIによる複数脊柱の撮影
- MRI and MRA of vessels acquired together
- MRI of the head and neck with specialized coils
- Direct radiography (DR) in a trauma patient: AP images, then move the patient once to acquire a set of orthogonal images, and then regroup by body part
- Sonographic evaluation of the kidneys and of the abdomen
- CT of the pelvis with CT angiographic runoff
- Angiographic studies of multiple vessels mixed with therapeutic interventions on selected segments.

Presentation of Group Procedures

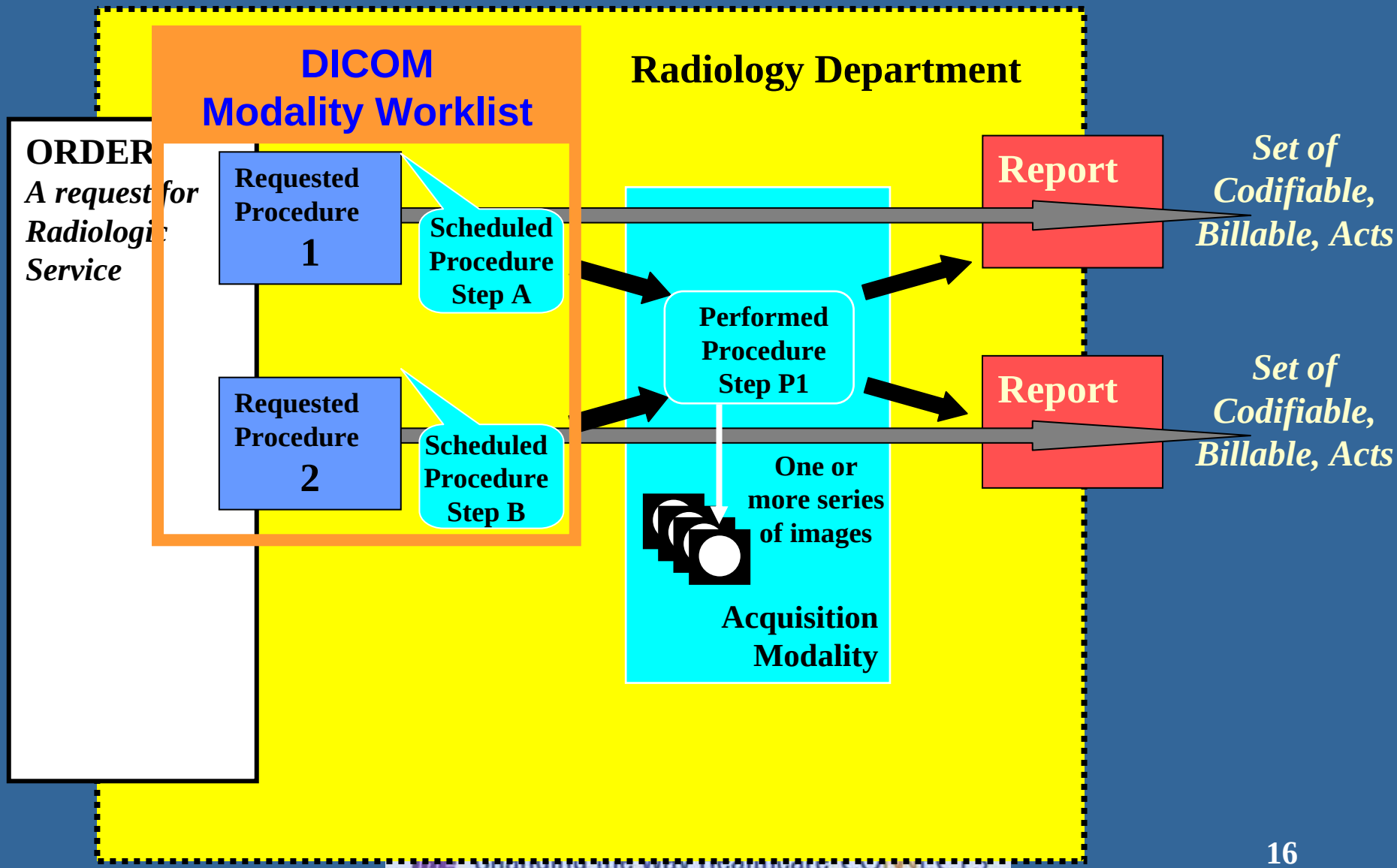
Scope

One Order – Two Procedures – **One Acquisition** - Two Reports

Step

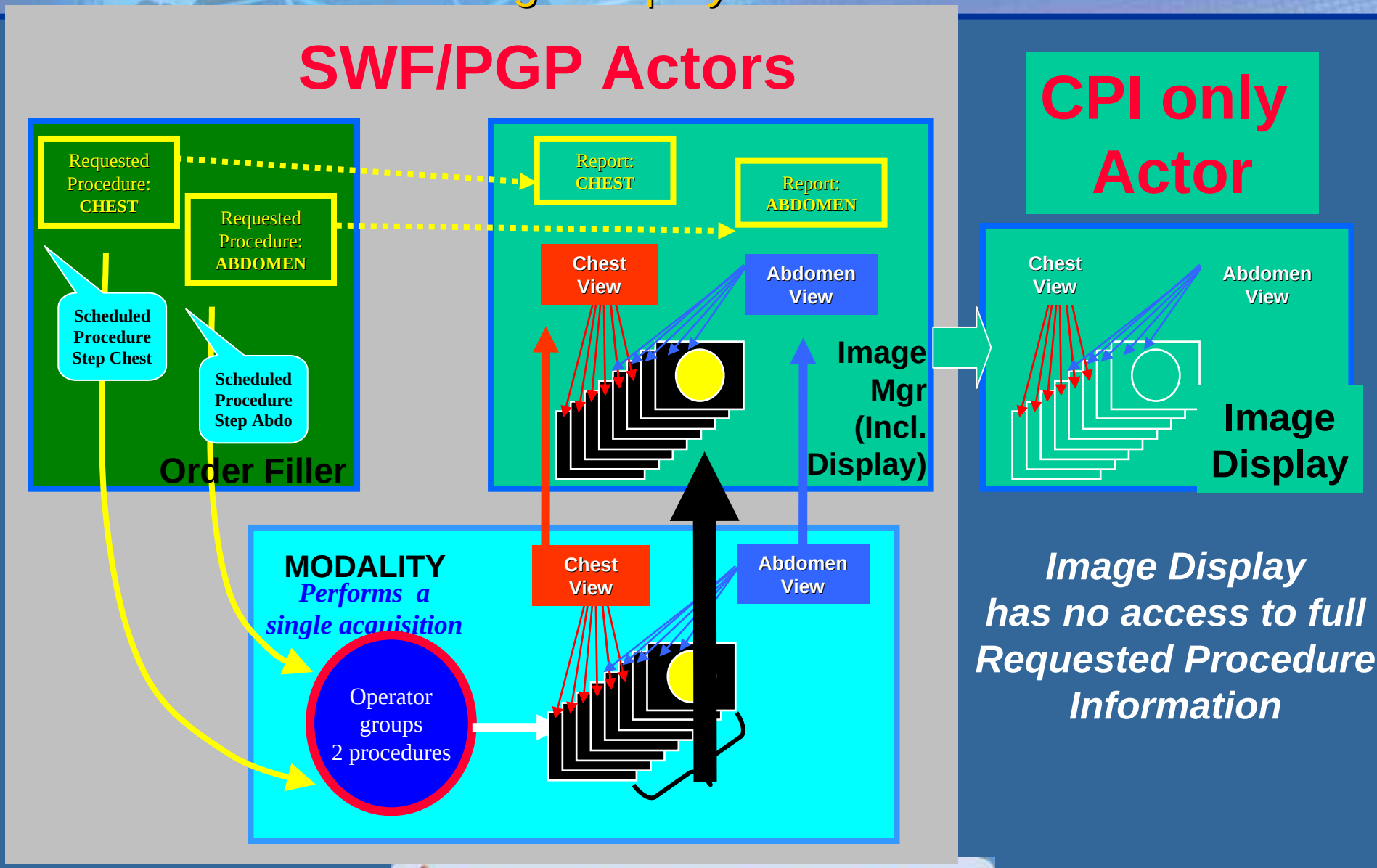


Group Case


DICOM
Modality Worklist
Radiology Department
ORDER
A request for
Radiologi
Service
Requested
Procedure
1
Scheduled
Procedure
Step A
Requested
Procedure
2
Scheduled
Procedure
Step B
Performed
Procedure
Step P1
One or
more series
of images
Acquisition
Modality
Report
Report
Set of
Codifiable,
Billable, Acts
Set of
Codifiable,
Billable, Acts

IHE PGP - Implementation Example

Image Display Constraints




放射線検査会計
Charge Posting
CHG

CHG

- アメリカでも誰も使っていないし、誰も説明してくれないので、省略します。

ティーチングファイルと臨床試験

Teaching File and Clinical Trail Export

TCE

TCE Profile: Abstract / Scope

Teaching Files are valuable training tools (mandated)

Clinical Trials are essential for research & evidence-based medicine

Assume you recognize a good study for Teaching or a Clinical Trial

- **How do you flag that study data?**
  - And add relevant notes
- **How do you get it properly de-identified?**
  - Teaching files (HIPAA Privacy)
  - Clinical trials (pseudonymization)
- **How do you route the study to the appropriate destination?**
  - Teaching File Authoring System
  - Clinical Trial Repository

- **Use existing DICOM mechanisms & infrastructure**

TCE Profile: Value for Customers

- **Digital Workflow for a traditionally film-based activity**
- **Facilitates clinical research and grant acquisition**
- **Standardizes clinical trial data collection**
- **Improves the efficiency of teaching file production**
- **Supports meeting teaching file requirements**
  - e.g. Accreditation Council on Graduate Medical Education

TCE Profile: Actors

Export Selector

- identifies information to be sent to a teaching file or clinical trial system
- e.g. a user function on a PACS diagnostic workstation
- can include images, reports, evidence documents, presentation states and additional information

Export Manager

- accepts selected objects
- de-identifies and re-identifies with pseudonymous values
- remaps to trial-specific identifiers and populates clinical trial specific attributes (Remap Identifiers option)
- sends pseudonymized DICOM objects and updated manifest to a Receiver.

Receiver

- a local teaching file
- a clinical trial repository
- a clinical trial system that transfers images to the central review facility


IHE
IHE Changing the Way Healthcare CONNECTS
WWW.IHE-J.ORG
WWW.IHE.NET