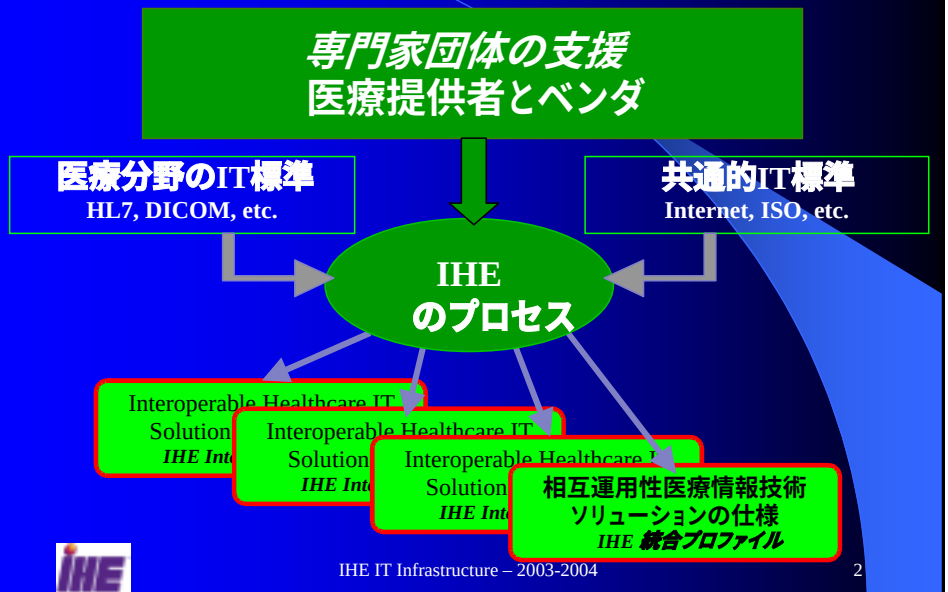
IHE IT Infrastructure Integrationの概要
Profiles 2003-2004

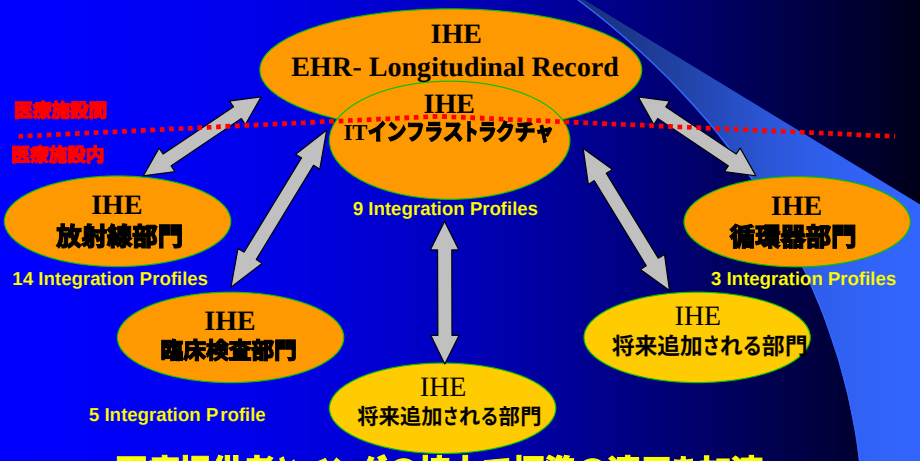
Charles Parisot, GE Healthcare IT
IHE IT Infrastructure Technical Committee co-chair
日本語訳　篠田 (東芝メディカルシステムズ)

IHEは保健医療システムの標準ベースの統合を進める



IHE 2004の成果と拡張スコープ

80以上のベンダが世界中で参加、4つのテクニカルフレームワーク
31統合プロファイル、毎年度のコネクタソンを実施、
世界中の主な展示会でのデモの実施

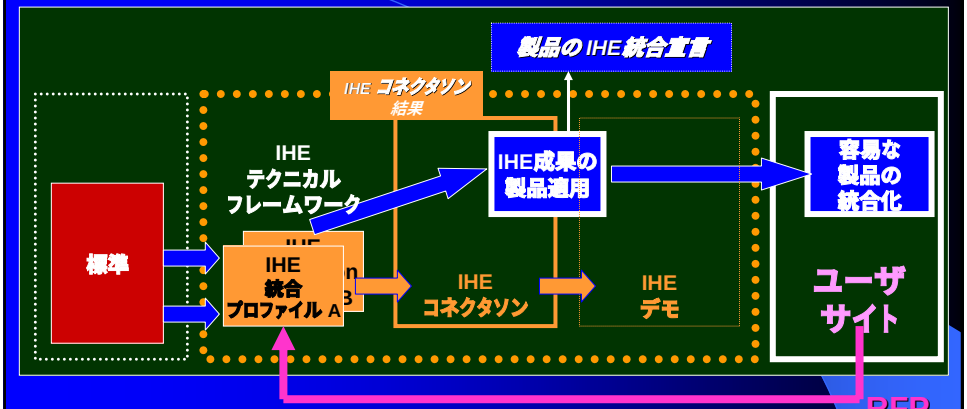


医療提供者とベンダの協力で標準の適用を加速

IHEのプロセス

- ユーザとベンダはともに作業し、システム統合上の課題を見つけ、そのソリューションを開発する
- 年次サイクルの集約的プロセス：
  - キーとなる診療のワークフローとシステム統合上の課題を見いだす
  - ソリューションを特定しそれに適用する標準の検討と選定を行う
  - IHEテクニカルフレームワークを記述し、レビューし、発行する
  - 「コネクタソン」により相互接続テストを行う
  - (HIMSS/RSNAなど)の展示会でデモを行う

実績のある標準の適用プロセス



- IHE統合プロファイルはIHEの神髄:
  - 個々の特定のシステム統合上の課題を解く、標準とオプションの詳細な選定
  - 発展的な診療提供者とベンダの合意に基づく効果的なソリューションのセット
  - ベンダは選択的に実装
  - ユーザは安定性を確保

ITインフラストラクチャについて もっと知るために

ITインフラストラクチャについてもっと知るためには:

Integrating the Healthcare Enterprise:

www.himss.org/ihe

IHEのパンフレットを読んで下さい！

http://www.himss.org/content/files/IHE_newsletter_final.pdf

IHE ITインフラストラクチャ2003-2004
5 統合プロファイルを完成

IHE IT インフラストラクチャ
2004-2005

IHE IT Infrastructure
5 Integration Profiles

表示のための情報検索

概要／スコープ

- 患者情報への簡単で迅速なアクセス
- よく使われる表示フォーマット（CDA、PDF、JPEGなど）の既存の保存されたドキュメントへのアクセス
- 医師へ提示するためにキーとなる患者中心の情報（アレルギー情報、現在の服薬情報、レポートのサマリなど）へアクセス
- 他のプロファイルであるEUA（エンタープライズユーザ認証）とPIX（患者同期アプリケーション）とのリンク

表示のための情報検索

価値命題：

- ユーザの便宜：
  - 医療提供者は情報を「見る」ことができる。重要な統合のステップ。
  - ユーザのスクリーン上のワークプレースやアプリケーションからのワークフロー。
  - 患者に同期したアプリケーションに対して複数かつ同時のアプリケーションワークフローを補完する。
- 情報への広範なエンタープライズにわたるアクセス：
  - 単純なクライアントに対してWeb技術を適用
  - 臨床データを保有する情報源では当然と考えられる臨床データの操作

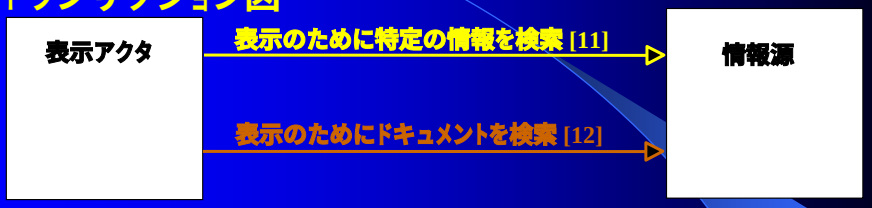
表示のための情報検索

キーとなる技術的特性：

- 利用される標準：
  - Webサービス (HTTP Getを用いる WSDL)。
  - 汎用IT表示フォーマット：XHTML, PDF, JPEG plus CDA L1.
  - クライアントは市販ブラウザや表示アプリ。
- 二つのサービス：
  - 特定の情報の検索：
    - 患者中心 ：患者ID
    - 依頼のタイプ (次のスライドを参照)
    - 日付、時間、最も最近のn個のデータ
  - ドキュメントの検索
    - オブジェクトの単一実例ID (OID)
    - 依頼のタイプ
    - 期待される内容タイプ

表示のための情報検索

トランザクション図



依頼のタイプ

- 全てのレポートのサマリ
- 臨床検査レポートのサマリ
- 画像検査レポートのサマリ
- 循環器レポートのサマリ
- 手術レポートのサマリ
- 集中治療レポートのサマリ
- 救急レポートのサマリ
- 退院レポートのサマリ
- アレルギーリスト
- 処方リスト

保存ドキュメント

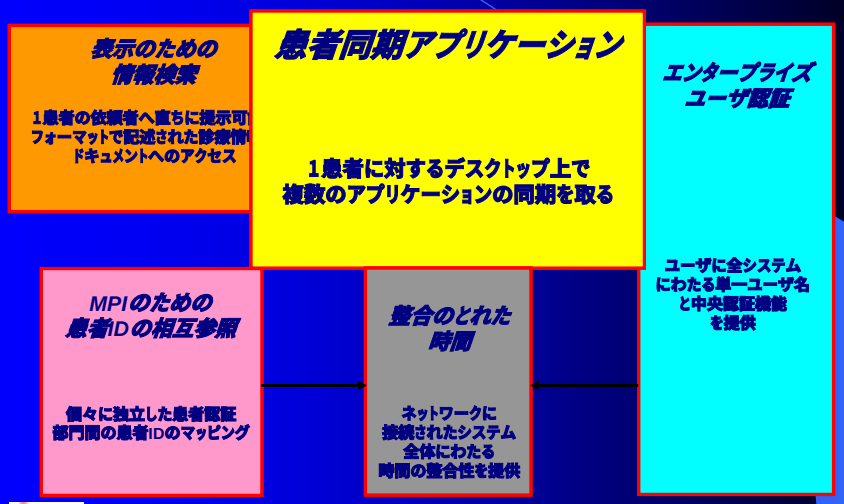
問い合わせキー – トランザクション [11] 表示のために特定の情報を検索

パラメータ名	必要性	記述
Request Type	R	依頼のタイプは、どのようなタイプの情報が回作されるべきかを指定。このパラメータは常に値をもっていなければならない。
Patient ID	R	この属性は問い合わせされる結果の主題を識別する。その値は認証局によるIDを持つ。
lowerDate Time	O	情報生成の最も前の日時の条件を示すために使用。
upperDate Time	O	情報生成の最も最近の日時の条件を示すために使用。
MostRecentResults	R	応答に含まれる最も直近の結果の数を指定するための数値。すなわち、1は最も最近の結果を提供することを意味する。

問い合わせキー – トランザクション [12]
表示のためのドキュメントの検索

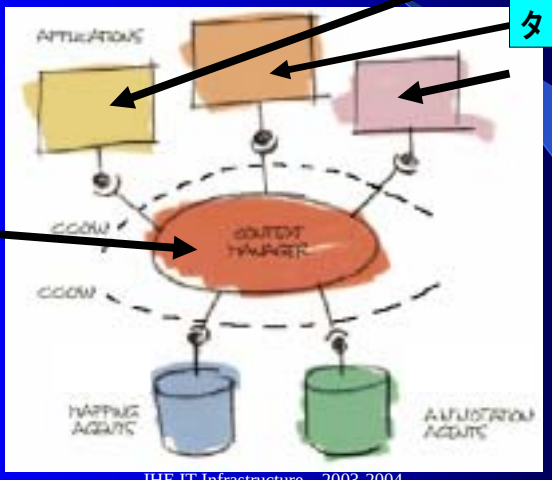
パラメータ名	必要性	記述
Request Type	R	このパラメータは、“DOCUMENT”なる値を持つことが要求される。.
Document UID	R	両アクタの双方に既知のドキュメントのUID。
PreferredContentType	R	このパラメータは、提供されるべきドキュメントのフォーマットを指定するために必須。(たとえば MIME content type).

IHE ITインフラストラクチャ
5統合プロファイル



IHE アクタの概念

患者コンテクスト参加アクタ



コンテクスト管理アクタ

患者同期アプリケーション

概要／スコープ

- 複数の様々なアプリケーションについて患者同期を取る
- 単一の患者を選定
- PIXプロファイルとともに利用されたとき、患者を指定して情報を利用する部門間の同期が得られる。

患者同期アプリケーション

価値命題：

- ユーザの便宜：
  - 各アプリケーションで患者を選択するという繰り返しの作業が必要なくなる
  - ユーザに、診療のワークフローにおける最も適切で、最もなじむ、アプリケーションにおける患者の選択をサポート
- 患者安全：
  - 同一の患者に対してアプリケーションにわたる全てのデータの参照を保証

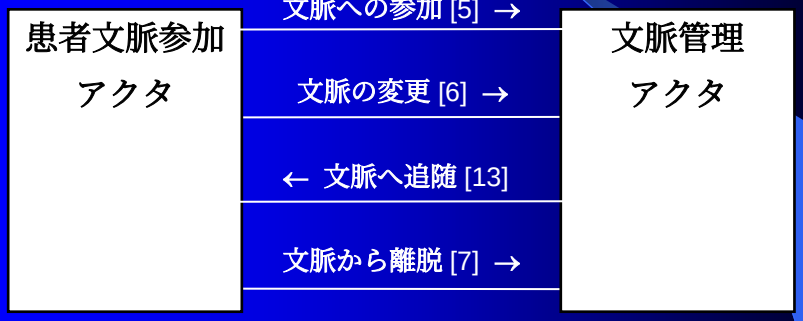
患者同期アプリケーション

キーとなる技術的特性：

- 利用される標準：
  - HL7の文脈依存管理標準である「CCOW」Version 1.4
  - WindowsとWeb技術の両方をサポート
  - 「患者に関する」をサポート
- IHE における制約：
  - *Patient.Id.IdList* 項目の使用を指定
    - PIXプロファイルとの最大限の相互運用性を保証
    - 患者ID項目 (HL7 2.3.1, 2.4, 2.5, CCOW)の起こりうる不整合に対して保護をかける

患者同期アプリケーション

トランザクション図



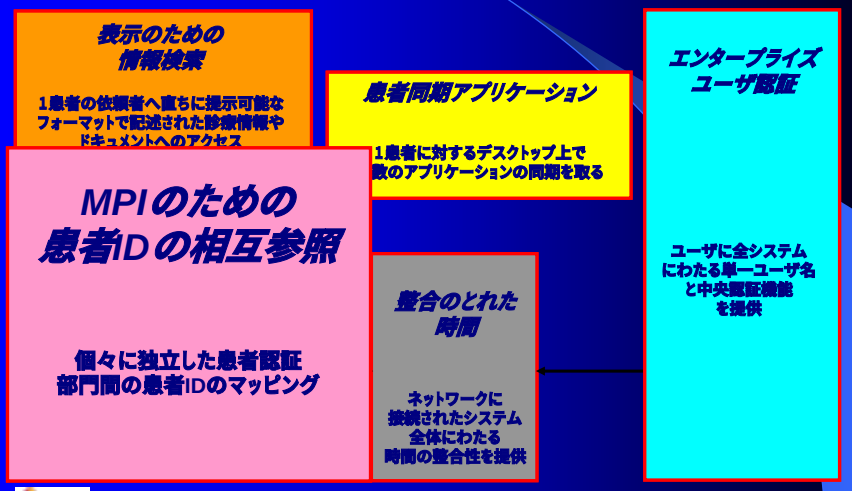
様々な技術の橋渡し
Sentillion HIMSS 2003

様々な技術の橋渡し
CareFX HIMSS 2004

異なるベンダによる異なるアプリケーションを一つにまとめて作動させる

- 診療提供者に様々なアプリケーションによる患者情報へ同期してアクセスできるようにする
- 施設内にわたって、診療提供者のためにワークフローをドラマチックに向上
- 診療提供者の満足度と生産性を向上
- 「単一患者を選択」を通じて患者安全を向上し、リスクを低減する

IHE ITインフラストラクチャ 5 統合プロファイル



患者ID相互参照機能

概要／スコープ

- 院内の全医療従事者が、それぞれの領域で患者のために利用するIDを登録することを可能とする
- その患者の診療サービスの目的のために、そのシステムに他のシステムのIDを問い合わせることを作業をサポート
- オプションで、他のシステムが患者のIDを更新した場合にそのシステムへ通知を行うことも可能

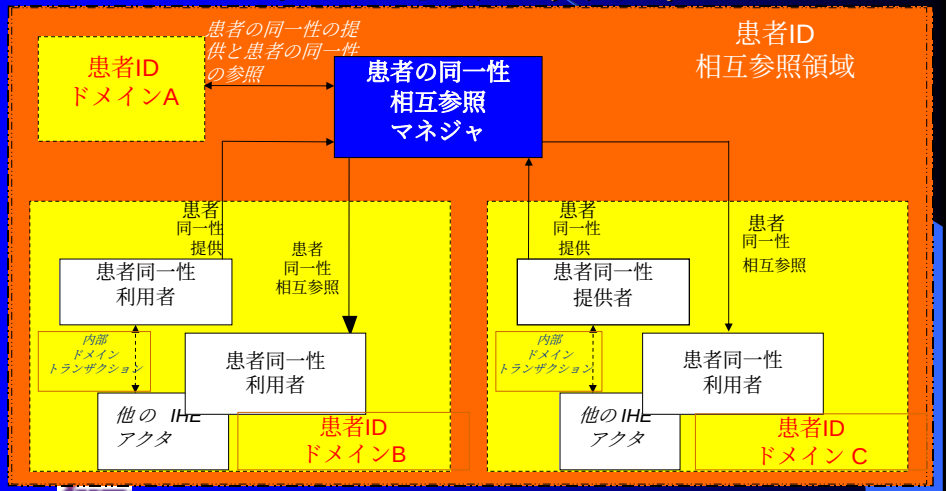
患者ID相互参照機能

価値命題

- 一カ所である患者の、全てのシステム内のIDを保守
- 別々にIDを発行された領域にわたり、患者のマッチングを行う任意の（カプセル化された）アルゴリズムを利用することは可能
- システムにまたがりデータの同期を図るためのより低コスト機能
  - 既存システムにIDとフォーマットの変更を求めない
- IHEで既に利用されている規格とトランザクションを利用

患者ID相互参照機能

ID ドメインとトランザクション



患者ID相互参照機能

キーとなる技術的特性

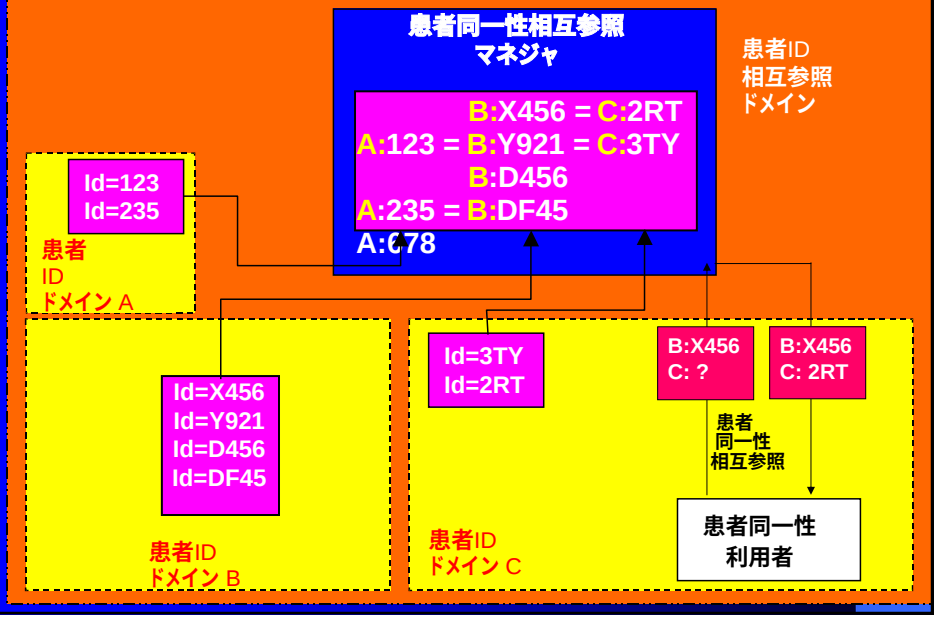
利用される規格

- HL7 Version 2.3.1とVersion 2.4
  - ADT 登録と更新トリガーイベント
    - A01: 入院登録
    - A04: 外来登録
    - A05: 入院前
    - A08: 患者更新
    - A40: 患者合併
  - 対応するIDの問い合わせ (ADT^Q23/K23)
  - IDリスト更新の通知 (ADT^A31)

キー特性

- ADTs は当該ドメインのメッセージ
- マスタとなるIDやMRNには適用されない。他のIDドメインでサポートされる

患者ID相互参照機能



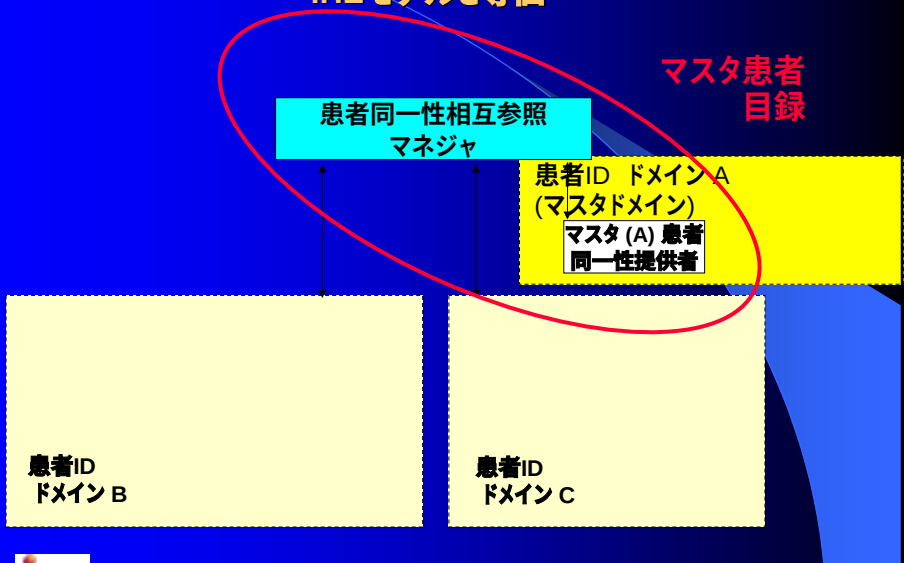
患者ID相互参照機能
キーとなる効果

- マスタ患者IDを必要としない (法的制約を容易にする)
- PIXマネジャは統合した患者情報を生成する必要がない
- どの患者IDドメインもマスタ患者IDを生成しているとみなすことができる (次のスライド参照)
- 患者情報はADTsアクタの責任範疇に入る。患者登録の分散化 (たとえば、RadとLab)に加えて、患者情報問い合わせ統合プロファイルが計画されている

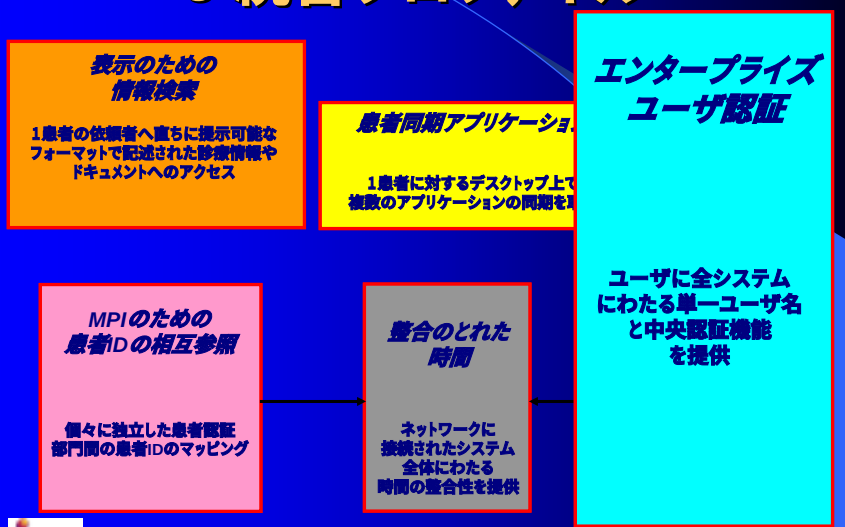
PIX 統合プロファイルとMIP
典型的な姿

PIX 統合プロファイルとMIP

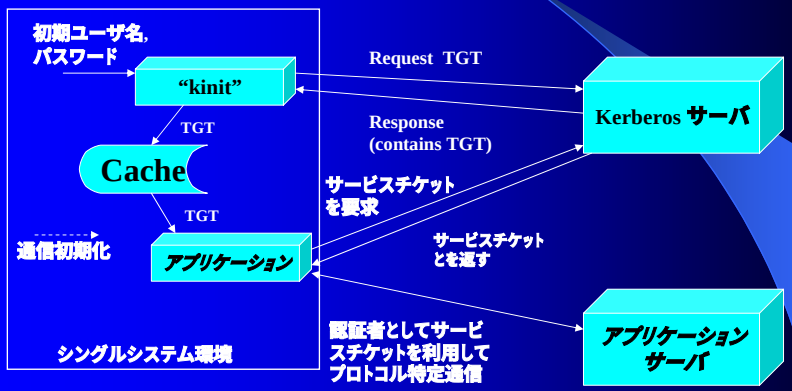
IHEモデルと等価



IHE IT インフラストラクチャ
5 統合プロファイル



施設内ユーザ認証
Kerberos認証



施設内ユーザ認証
概要／スコープ

- 単一の施設は、単一のセキュリティポリシのセットで管理され、共通のネットワークドメインを持つようサポートする
- 診療施設の全ての機器やソフトウェアで有効な一ユーザー氏名を保証
- 集中化されたユーザ認証管理を提供
- ユーザにシングルサインオン機能を提供

施設内ユーザ認証
価値命題

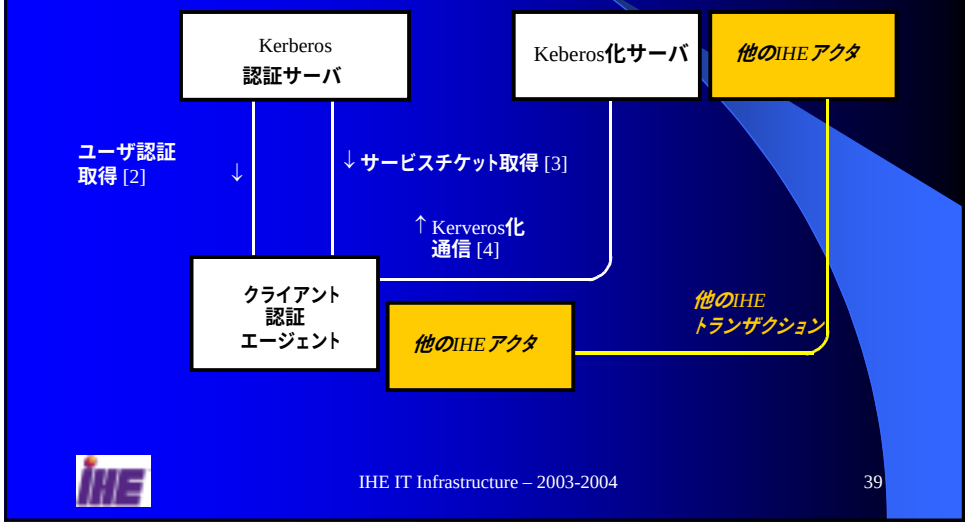
- 始めにありきアクセス管理
  - 多くのアプリやデータアクセス操作に対して、ユーザ認証は必須
- コストの低減／封じ込め
  - ユーザ認証管理を集中化
  - マルチベンダによるシステム実装を簡素化
- ユーザに対してワークフローの改善を提供
  - ユーザの受け入れやすさ助長
  - 非効率なユーザの仕事切り替え時間を低減
- セキュリティプロテクションの保証レベルを向上.

施設内ユーザ認証
キーとなる技術特性

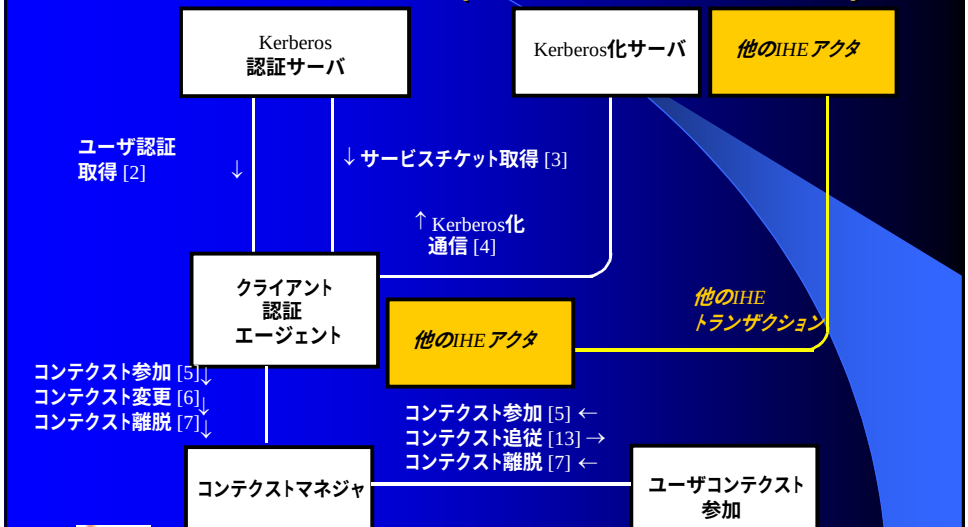
利用される標準
- Kerberos v5 (RFC 1510)
  - 1993年から安定的に使用
  - 現在のOSプラットフォームに広く実装
  - その10年の歴史で攻撃には上手く持ちこたえた
  - 全てのプラットフォームに完全に相互運用性を保証
- HL7のCCOWユーザ主題

最小のアプリケーションの変更
- アプリケーション特定、非相互運用的認証の排除
- 低安全でプロプライエタリなセキュリティ技術の置き換え

施設内ユーザ認証
トランザクション図



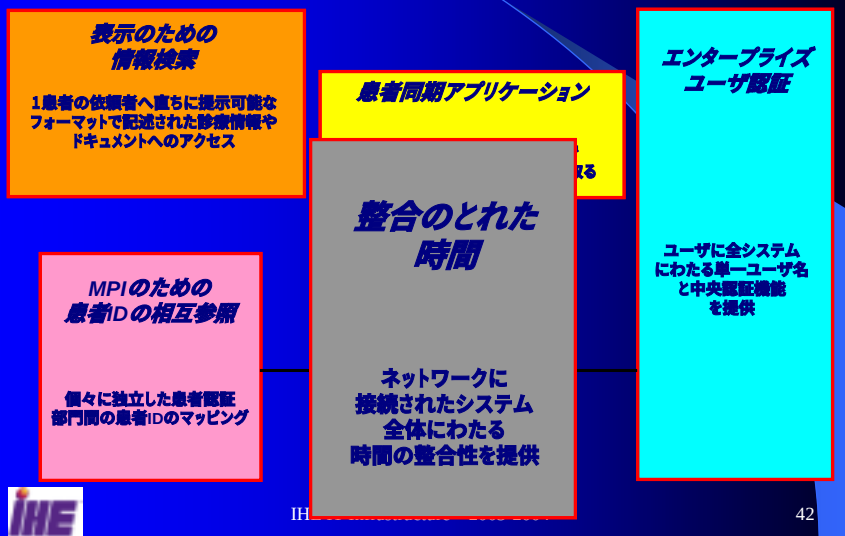
施設内ユーザ認証
トランザクション図 (+CCOWオプション)



施設内ユーザ認証
キーとなる効果

- Kerberos化サーバと認証サーバとの間でトランザクションが必要ないのでオーバヘッドが限定的(単に適当な証明書の設定することのみ)
- 任意の認証技術と連動するKerberosプロトコルが定義。多様な認証技術(トークン、バイオメトリック技術、ICカード)をサポート。独自コンポーネント対ーユーザワークステーション上に一つと認証サーバ上のマッチングコンポーネントーを特定実装として必要。ユーザ認証が完了すれば、継続するKerberosトランザクションは同様。

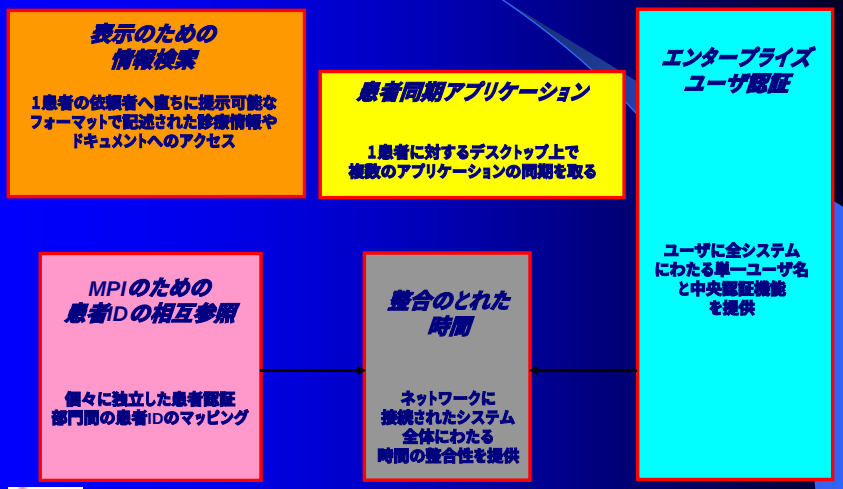
IHE IT インフラストラクチャ
5 統合プロファイル



整合の取れた時間
スコープと価値命題

- ネットワーク内の多くのコンピュータのシステムクロックとタイムスタンプが同期することを保証
- 中間値誤差で1秒以下は多くの目的で十分な精度
- 整合の取れた時間プロファイルは、RFC1305で定義されたNetwork Time Protocol (NTP)の利用を指定

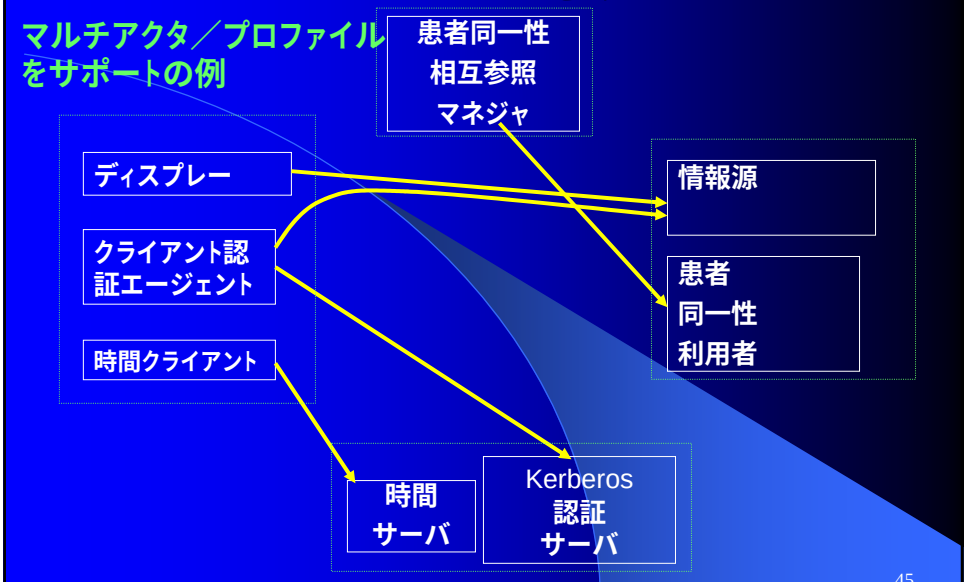
IHE IT インフラストラクチャ
5 統合プロファイル



IHE IT 統合プロファイル間の相乗効果

EUA/CT & PIXとのRID

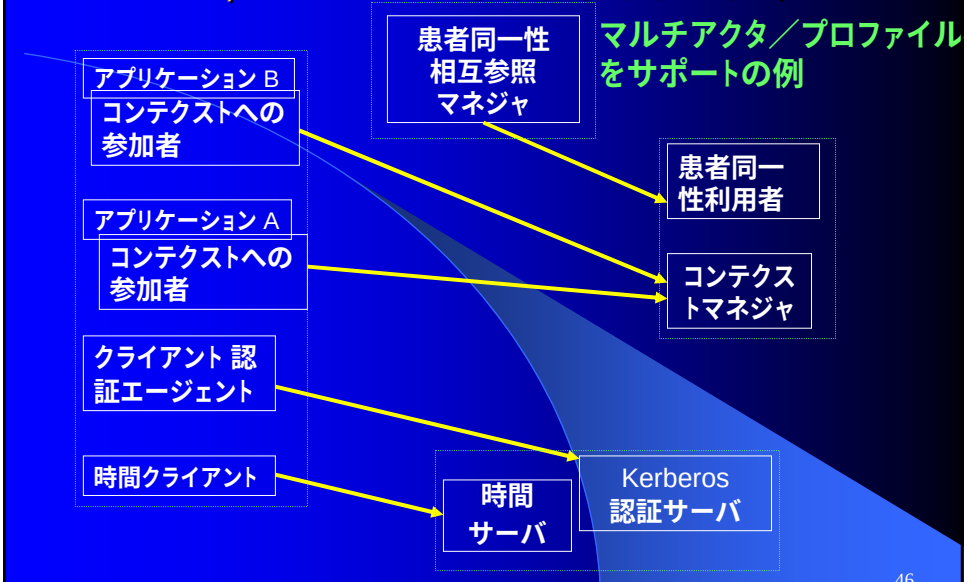
マルチアクタ／プロファイル
をサポートの例



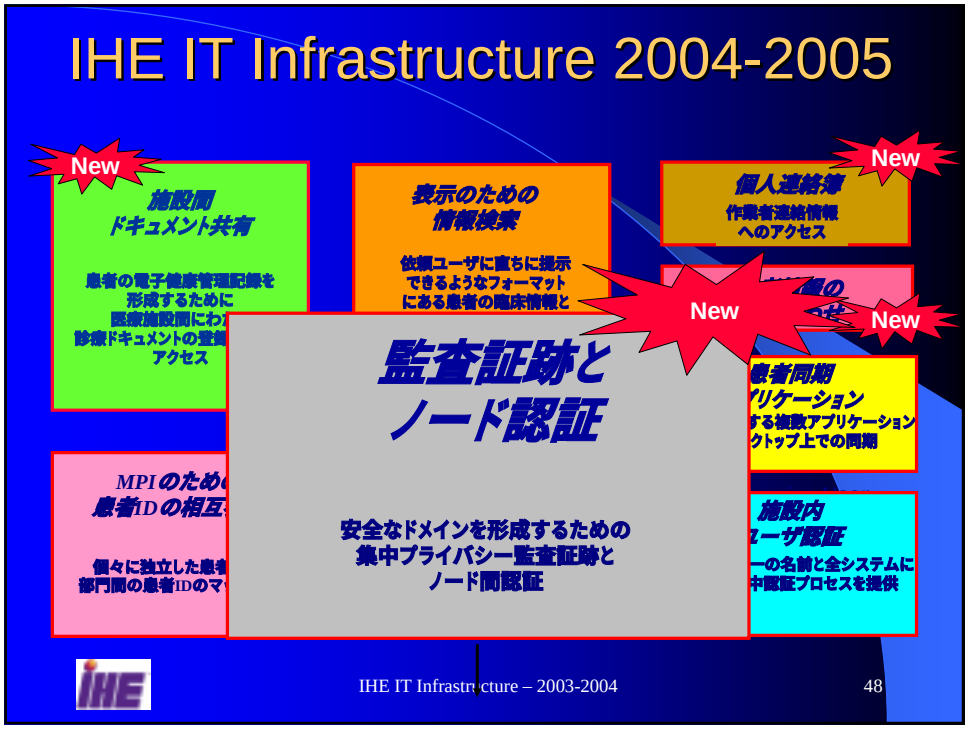
IHE IT 統合プロファイル間の相乗効果

PSA, EUA & PIXとのアプリケーション

マルチアクタ／プロファイル
をサポートの例




IHE IT インフラストラクチャ
2004-2005
New
施設間
ドキュメント共有
患者の電子健康管理記録を
形成するために
医療施設間にわたる
診療ドキュメントの登録と配布と
アクセス
表示のための
情報検索
依頼ユーザに直ちに提示
できるようなフォーマット
にある患者の臨床情報と
ドキュメントにアクセス
New
個人連絡簿
作業者連絡情報
へのアクセス
患者情報の
問い合わせ
New
New
患者同期
アプリケーション
一患者に対する複数アプリケーション
のデスクトップ上での同期
New
監査証跡と
ノード認証
安全なドメインを形成するための
集中プライバシー監査証跡と
ノード間認証
MPIのための
患者IDの相互参照
個々に独立した患者識証
部門間の患者IDのマッピング
施設内
ユーザ認証
ユーザに単一の名前と全システムに
わたる集中認証プロセスを提供
整合性の取れた時間
ネットワーク接続されたシステムに
わたる時間の調整
IHE
IHE IT Infrastructure – 2003-2004
47


IHE IT Infrastructure 2004-2005
New
施設間
ドキュメント共有
患者の電子健康管理記録を
形成するために
医療施設間にわ
診療ドキュメントの登
アクセス
表示のための
情報検索
依頼ユーザに直ちに提示
できるようなフォーマット
にある患者の臨床情報と
New
個人連絡簿
作業者連絡情報
へのアクセス
New
New
患者同期
アプリケーション
する複数アプリケーション
クトップ上での同期
監査証跡と
ノード認証
安全なドメインを形成するための
集中プライバシー監査証跡と
ノード間認証
MPIのため
患者IDの相互
個々に独立した患
部門間の患者IDのマ
施設内
ユーザ認証
一の名前と全システムに
中認証プロセスを提供
IHE
IHE IT Infrastructure – 2003-2004
48

IHE と HIPAA のセキュリティ

- **ユーザ同一性** → PWP, EUA
- **ユーザ認証** → EUA
- **ノードの認証** → ATNA
- **セキュリティ監査証跡** → ATNA
- **データの完全性管理** → CT, ATNA TLS option
- **データの守秘性** → ATNA TLS option
- **アクセス管理** → IHEロードマップの将来項目

スコープ

- 医療機関のセキュリティとプライバシーに係わる部分で利用される個々のシステムに対して、基本的なセキュリティ機能を定義
- IHE放射線部門の基本セキュリティプロファイル（2002年）の他の医療分野における利用への拡張
- ネットワーク環境の二つのカテゴリをサポート
- 認証のそれぞれの種類のプロファイル類の最初の部分

ATNA プロファイル
価値命題

- 患者のプライバシーとシステムのセキュリティを保護：
  - 倫理的かつ法的要請に対応
- 施設の管理上の便宜：
  - 統合され、一様な監査システム
  - マルチベンダ間で共通する手法で施設としてのポリシとプロトコルを簡素化
  - 共通手法は管理業務を簡素化
- コードの再利用で開発費や支援費を削減：
  - ベンダに対して、複数のアクタをサポートする際に、単一の開発で対応できるように支援
  - 様々なセキュリティポリシと法的規制から来る必要性をサポートするに際して、単一の開発努力で対応可能とする

セキュリティ要求

- 理由：臨床上の利用とプライバシー
  - 認可を受けた人だけが患者の医療データにアクセスすべきで、情報は他には公開されるものではない
  - 認可を受けていない人が操作やデータの更改に干渉することが許されるべきではない
- 手続きとセキュリティメカニズムにより、以下を保証：
  - 守秘性
  - 完全性
  - 可用性
  - 信頼性

セキュリティ措置

- Authentication:
  Establish the user and/or system identity, answers question:
  "Who are you?"
  - ATNA defines: How to authenticate network connections.
  - ATNA requires: System internal authentication mechanisms, e.g. Enterprise User Authentication (EUA).
- Authorization and Access control
  Establish user's ability to perform an action,
  e.g. access to data, answers question:
  "Now that I know who you are,
  what can you do?"
  - ATNA defines: How to authorize network connections.
  - ATNA requires: System internal mechanisms for both local and network access.

セキュリティ措置

- Accountability and Audit trail
  Establish historical record of user's or system actions over period of time, answers question:
  What have you done?"
  - ATNA Defines: Audit message format and transport protocol

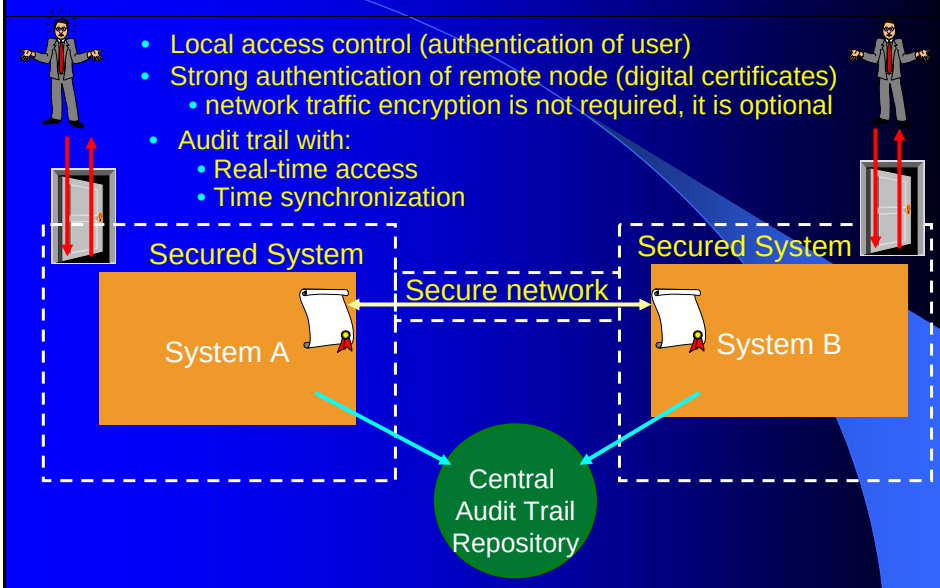
IHE Goal

IHE makes cross-node security management easy:

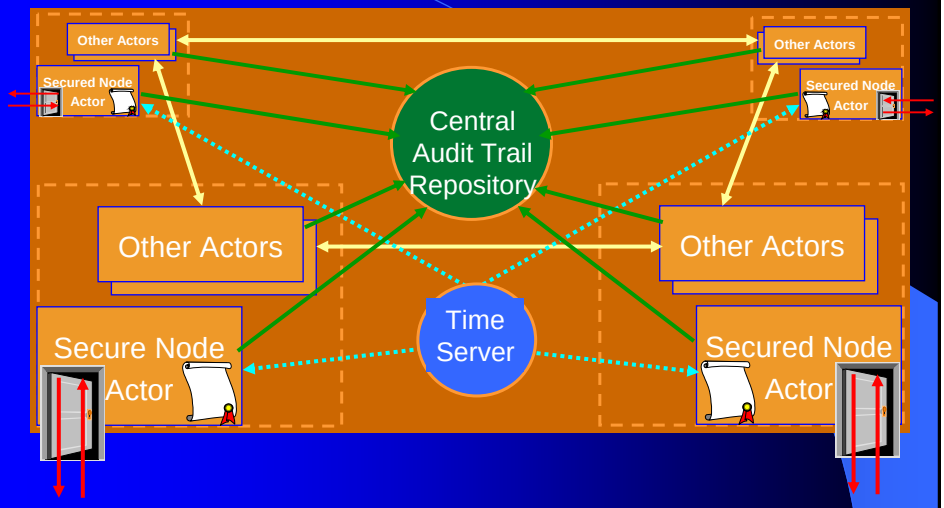
- Only a simple manual certificate installation is needed.
- Separate the authentication, authorization, and accountability functions to accommodate the needs of different approaches.
- Enforcement driven by 'a posteriori audits' and real-time visibility.

Integrating trusted nodes

- Local access control (authentication of user)
- Strong authentication of remote node (digital certificates)
  - network traffic encryption is not required, it is optional
- Audit trail with:
  - Real-time access
  - Time synchronization



Secured Domain: integrating trusted nodes



Network Environments

- Physically secured networks
  - Explicit physical security preventing access by other nodes, or
  - VPN and VLAN technologies that provide equivalent network isolation.
- Protected networks
  - Physical security that prevents modification or installation of unauthorized equipment
  - The network is shared with other authorized nodes within the enterprise that should not have unrestricted access to patient information.
- Unprotected networks
  - Not generally supported, although nodes with sufficient node level security and using encryption may be safe.

Node Security

- ATNA specifies some of the capabilities that are needed, e.g. access control.
- ATNA does not specify policies
- ATNA does not specify mechanisms, although other IHE protocols like EUA are obvious candidates.
- This permits vendors and enterprises to select technologies and policies that are appropriate to their own purposes without conflicting with the ATNA profile.

Auditing System

- Designed for surveillance rather than forensic use.
- Two audit message formats
  - IHE Radiology interim format, for backward compatibility with radiology
  - IETF/DICOM/HL7/ASTM format, for future growth
    - DICOM Supplement 95
    - IETF Draft for Common Audit Message
    - ASTM E.214
    - HL7 Audit Informative documents
  - Both formats are XML encoded messages, permitting extensions using XML standard extension mechanisms.

IHE Audit Trail Events
Combined list of IETF and DICOM events

Actor-start-stop	*The starting or stopping of any application or actor.*
Audit-log-used	*Reading or modification of any stored audit log*
Begin-storing-instances	*The storage of any persistent object, e.g. DICOM instances, is begun*
Health-service-event	*Other health service related auditable event.*
Images-availability-query	*The query for instances of persistent objects.*
Instances-deleted	*The deletion of persistent objects.*
Instances-stored	*The storage of persistent objects is completed.*

IHE Audit Trail Events
Combined list of IETF and DICOM events

Medication	*Medication is prescribed, delivered, etc.*
Mobile-machine-event	*Mobile equipment is relocated, leaves the network, rejoins the network*
Node-authentication-failure	*An unauthorized or improperly authenticated node attempts communication*
Order-record-event	*An order is created, modified, completed.*
Patient-care-assignment	*Patient care assignments are created, modified, deleted.*
Patient-care-episode	*Auditable patient care episode event that is not specified elsewhere.*
Patient-record-event	*Patient care records are created, modified, deleted.*

IHE Audit Trail Events
Combined list of IETF and DICOM events

PHI-export	***Patient information is exported outside the enterprise, either on media or electronically***
PHI-import	***Patient information is imported into the enterprise, either on media or electronically***
Procedure-record-event	***The patient record is created, modified, or deleted.***
Query-information	***Any auditable query not otherwise specified.***
Security-administration	***Security alerts, configuration changes, etc.***
Study-object-event	***A study is created, modified, or deleted.***
Study-used	***A study is viewed, read, or similarly used.***

Authenticate Node transaction

- X.509 certificates for node identity and keys
- TCP/IP Transport Layer Security Protocol (TLS) for node authentication, and optional encryption
- Secure handshake protocol of both parties during Association establishment:
  - Identify encryption protocol
  - Exchange session keys
- Actor must be able to configure certificate list of authorized nodes.
- ATNA presently specifies mechanisms for HTTP, DICOM, and HL7

Record Audit Event transaction

- Reliable Syslog (RFC 3195) is the preferred transport for Audit Records, although BSD Syslog protocol (RFC 3164) is permitted for backward compatibility with Radiology Basic Security.
- Audit trail events and content based on IETF, DICOM, HL7, and ASTM standards. Also, Radiology Basic Security audit event format is allowed for backward compatibility.

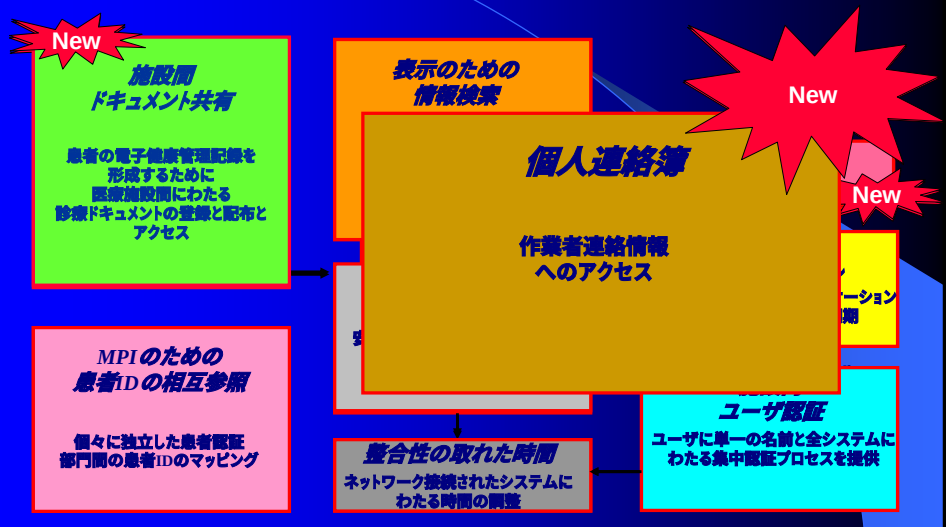
Maintain Time transaction

- Network Time Protocol (NTP) version 3 (RFC 1305) for time synchronization
- Actor must support manual configuration
- Required accuracy: 1 second
- Optionally Secure NTP may be used

What it takes to be a secure node

- The Secure node is not a simple add-on of an auditing capability. The larger work effort is:
  - Instrumenting all applications to detect auditable events and generate audit messages.
  - Ensuring that all communications connections are protected.
  - Establishing a local security mechanism to protect all local resources.
  - Establishing configuration mechanisms for:
    - Time synchronization
    - Certificate management
    - Network configuration
- Implement the audit logging facility

IHE IT Infrastructure 2004-2005



Personnel White Pages (PWP) – Abstract/Scope

- Provide access to basic information about the human workforce members
  - Does not include Patients
- Defines method for finding the PWP
- Defines query/access method
- Defines attributes of interest

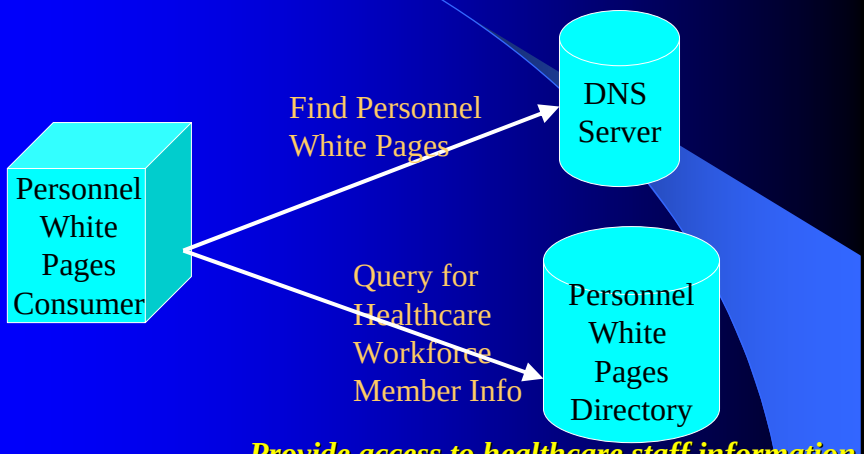
Personnel White Pages (PWP) – Value Proposition

- Single Authoritative Knowledge Base
  - Reduce duplicate and unconnected user info database
  - Single place to update
    - Name Changes
    - New Phone Number
    - Additional Addresses
- Enhance Workflow and Communications
  - Providing information necessary to make connections
    - Phone Number
    - Email Address
    - Postal Address

Personnel White Pages (PWP) – Value Proposition

- Enhance User Interactions
  - Provide user friendly identities and lists
    - List of members
    - Displayable name of a user
    - Initials query
- Contributes to Identity Management
  - Additional methods of identity cross verification
    - Name, address, phone number, email
    - Cross reference with Enterprise User Authentication identity
  - Future expansion likely will contain certificates

PWP - Transactions



Provide access to healthcare staff information to systems in a standard manner.

PWP - Key Technical Properties

- DNS – Service discovery transaction
- LDAP – Personnel White Pages Query
  - LDAP v3
  - Use of UTF-8 to support global character sets
  - Method for determining the Base DN for PWP
- Directory of Attributes
  - inetOrgPerson – RFC 2789
  - X.500 Person – RFC 2256
  - Recommended attributes to be filled if available
- Healthcare specifics
  - Names using HL7 naming complex
  - Support for Language specific names
  - IHE Enterprise User Authentication (EUA) user ID
  - Universal Physician Identification Number (UPIN)

PWP – Typical Uses

- Clinical user logs into an acquisition device. The clinical application queries the directory using the user's username and displays the user's full name.
  - The system further supports the display of the user's Asian complexes
- A Clinical application queries for user's organization identification to embed in a new data report.

PWP – Typical Uses

- The user needs to send a report to the email address of a colleague. The application allows the user to search for that user's information, and selects the target user's email address.
- The user reviews an existing report and finds initials. The system queries on the initials found in the report and displays the displayable name.
- The user is reviewing a structured report with an embedded author's universal provider ID. This universal provider ID is used in a query to find the author of the report. The user calls the author on the phone to review the report details.

Personnel White Pages (PWP) – Shall Include

- Login Id, johnmk, q1234 moehrkj@krb.local
- Last Name, Moehrke
- Display Name, John F. Moehrke
- Other Unique Identifiers (e.g. professional).

Personnel White Pages (PWP) – Shall Include if available

- First Name, John
- Initials, JFM
- Phone Numbers, (555) 293-1667
- Title, Systems Engineer
- Email Address, John.Moehrke@med.ge.com
- Postal Address, W126 N7449 Flint Rd
- Postal Code 53051
- Manager, and Charles Parisot
- Employee Type Intern
- Etc…

Personnel White Pages (PWP) – May Include

- Department affiliation,
- Secretary,
- Photo ID,
- Etc…

Personnel White Pages (PWP) – Discourages

Directory definitions that are no longer relevant or useful. This does not prohibit the use.

- Passwords
- Audio – obsolete format
- Telegram destination Indicator
- ISDN Number
- Telex Number
- Etc…

Personnel White Pages (PWP) – Globalization

- Leverage LDAP use of UTF-8
- Language tag – allows for different names based on language written/spoken
- HL7 Name Data Type (XCN)

givenname: XiaoDong
givenname;lang-cn: 小東
cn: Wang XiaoDong
cn;lang-cn: 王 小東
cn;lang-x-ihe: Wang^XiaoDong^^^^^^A~王^小東 ^^^^^^

PWP Example

objectclass: Top
objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
dn: cn=Wang XiaoDong, ou=Radiologists, o=Saint-ihe-hospital.local
cn: Wang XiaoDong
cn: XiaoDong, Wang, Florida Department of Health:123456789
cn;lang-cn: 王 小東
cn;lang-x-ihe: Wang^XiaoDong^^^^^^A~王^小東^^^^^^
sn: Wang
givenname: XiaoDong
givenname;lang-cn: 小東
sn;lang-cn: 王
ou: People
uid: XiaoDong
title: Sample HL7 person
mail: Wang.XiaoDong@foo.bar.com
telephonenumber: 555-555-5678

Integrating the Healthcare Enterprise

患者情報問い合わせ (PDQ) プロファイル

Mike Henderson
Eastern Informatics, Inc.
Co-chair, IHE IT Infrastructure Technical Committee

Patient Demographics Query
Abstract/Scope

- Allow quick retrieval of a patient list including common patient names, identifiers, contacts, and visit information
- Enable selection of correct patient when full identification data may not be available
- Limits access to only a subset of demographic and visit information

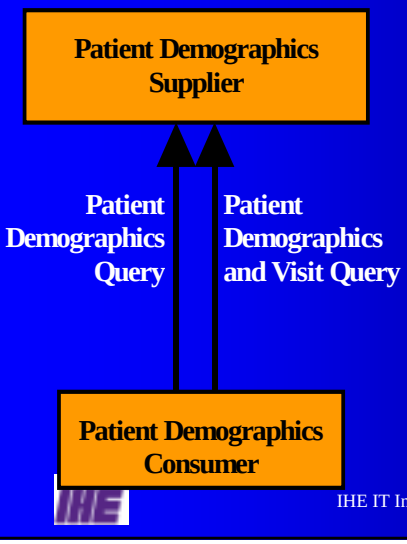
Patient Demographics Query
Value Proposition

- Enables access on demand to diverse systems and devices
  - Participants that do not need continual synchronization of patient registration information
  - Devices that cannot participate in monitoring of ADT feeds, *e.g.*:
    - Small-footprint devices
    - Low-memory devices

Patient Demographics Query
Value Proposition (cont'd)

- Allow search on full or partial data
- Retrieve information from any domain to which the client has query access
- Allows use of matching algorithm (*e.g.*, soundex) to find near matches

Patient Demographics Query
Transaction Diagram



A departmental system that is connected on demand to the registration system.

Diverse systems including bedside monitors, physician office systems, lab applications, mobile blood bank registries; might be any system at the point of contact.

Patient Demographics Query
Standards Used

- Employs HL7 Conformance Based Queries
  - Defined in HL7 Version 2.5, Chapter 5
  - Profiles Query by Parameter (QBP^Q22) with Segment Pattern Response (RSP^K22)

Patient Demographics Query
Actors

Patient Demographics Consumer

- Definition
  - Requestor of patient demographic (and perhaps current visit) information
  - Allows user to associate information with a patient at the point of care
- Transaction Supported – Required
  - Patient Demographics Query (as sender)
- Transaction Supported – Optional
  - Patient Demographics and Visit Query (as sender)

Patient Demographics Query
Actors

Patient Demographics Supplier

- Definition
  - Repository of patient information that can be searched on demographic or visit-related fields
- Transaction Supported – Required
  - Patient Demographics Query (as receiver)
- Transaction Supported – Optional
  - Patient Demographics and Visit Query (as receiver)

Patient Demographics Query
Operation

Patient Demographics Query

- User enters full or partial demographic information (*e.g.*, partial last name and first initial) for patients of interest
- Application associated with Patient Demographics Consumer sends HL7 QBP^Q22 to Patient Demographics Supplier to find matching information
  - May request specific domains from which to return identifier information

Patient Demographics Query
Operation (cont'd)

Patient Demographics Response – Patient Demographics Supplier recognizes Patient Identifier Domain(s) requested by Patient Demographics Consumer:

- Patient Demographics Supplier returns HL7 message with list of matches (if any) to Patient Demographics Consumer
  - Demographic information in HL7 PID and PD1 segments
    - From demographic source associated with receiving application
  - If no matches found, returns code **NF** (not found) in QAK-2-Query Status
- Application associated with Patient Demographics Consumer builds pick list from which user may select
  - Matches within level of tolerance defined by user
  - Query allows any matching algorithm the supplier may choose to make available

Patient Demographics Query
Operation (cont'd)

Patient Demographics Response – Patient Demographics Supplier does not recognize Patient Identifier Domain(s) requested by Patient Demographics Consumer:

- Patient Demographics Supplier returns code **AE** (application error) to Patient Demographics Consumer in the following fields
  - MSA-1-Acknowledgment Code
  - QAK-2-Query Response Status
- Patient Demographics Supplier returns one ERR segment to Patient Demographics Consumer for each unrecognized domain

Patient Demographics Query
Operation

Patient Demographics and Visit Query

- User enters full or partial demographic/visit information (*e.g.*, room/bed number) for patients of interest
- Application associated with Patient Demographics Consumer sends HL7 QBP^ZV1 to Patient Demographics Supplier to find matching information
  - May request specific domains from which to return identifier information

Patient Demographics Query
Operation (cont'd)

Patient Demographics and Visit Response – Patient Demographics Supplier recognizes Patient Identifier Domains requested by Patient Demographics Consumer:

- Patient Demographics Supplier returns HL7 RSP^ZV2 message with list of matches to Patient Demographics Consumer
  - Demographic information in HL7 PID and PD1 segments
  - Visit information in PV1 and PV2 segments
    - From demographic source associated with receiving application
  - If no matches found, returns code **NF** (not found) in QAK-2-Query Status
- Application associated with Patient Demographics Consumer builds pick list from which user may select

Patient Demographics Query
Operation (cont'd)

Patient Demographics and Visit Response – Patient Demographics Supplier does not recognize Patient Identifier Domain(s) requested by Patient Demographics Consumer:

- Patient Demographics Supplier returns code **AE** (application error) to Patient Demographics Consumer in the following fields
  - MSA-1-Acknowledgment Code
  - QAK-2-Query Response Status
- Patient Demographics Supplier returns one ERR segment to Patient Demographics Consumer for each unrecognized domain

Patient Demographics Query
Message Examples

Patient Demographics Query – Example Message:

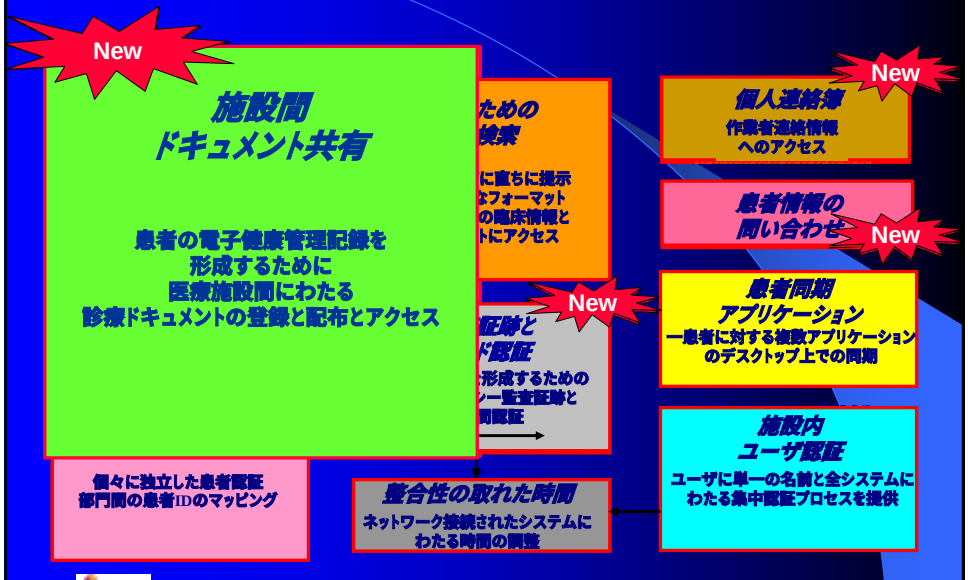
```
MSH|^&~¥|CLINREG|WESTCLIN|HOSPMPI|HOSP|1999121211
  35-0600||QBP^Q22^QBP_Q21|1|D|2.5
QPD|Q22^Find
  Candidates^HL70471|111069|@PID.5.1^SMITH~@PID.5
  .2^JOHN~@PID.8^M|80|MATCHWARE|1.2||^^^METRO
  HOSPITAL~^^^SOUTH LAB
RCP||I|20^RD
```

Patient Demographics Query
Message Examples (cont'd)

Patient Demographics Response – Example Message:

```
MSH|^&~¥|HOSPMPI|HOSP|CLINREG|WESTCLIN|199912121135-
   0600||RSP^K22^RSP_K21|1|D|2.5
MSA|AA|8699
QAK|111069|OK|Q22^Find Candidates^HL70471|3
QPD|Q22^Find Candidates^HL70471|111069|@PID.5.1^SMITH~
   @PID.5.2^JOHN~@PID.8^M|80|MATCHWARE|1.2||^^^METRO HOSPITAL~^^^SOUTH
   LAB|
PID|||66785^^^METRO HOSPITAL~66532^^^SOUTH
   LAB||Smith^John||19630423|M||C|N2378 South
   Street^^Madison^WI^53711|
QRI|95||MATCHWARE 1.2|
PID|||87443^^^METRO HOSPITAL~651189^^^SOUTH
   LAB||Smith^Jon||19470606|M||C|124 Second Street^^Madison^WI^53711|
QRI|90||MATCHWARE 1.2|
PID|||43266^^^METRO HOSPITAL~81209^^^SOUTH
   LAB||Smithy^John||19901210|M||C|W11234 Bay Drive^^Lodi^WI^53555|
QRI|85||MATCHWARE 1.2|
```


IHE IT Infrastructure 2004-2005



Introduction:

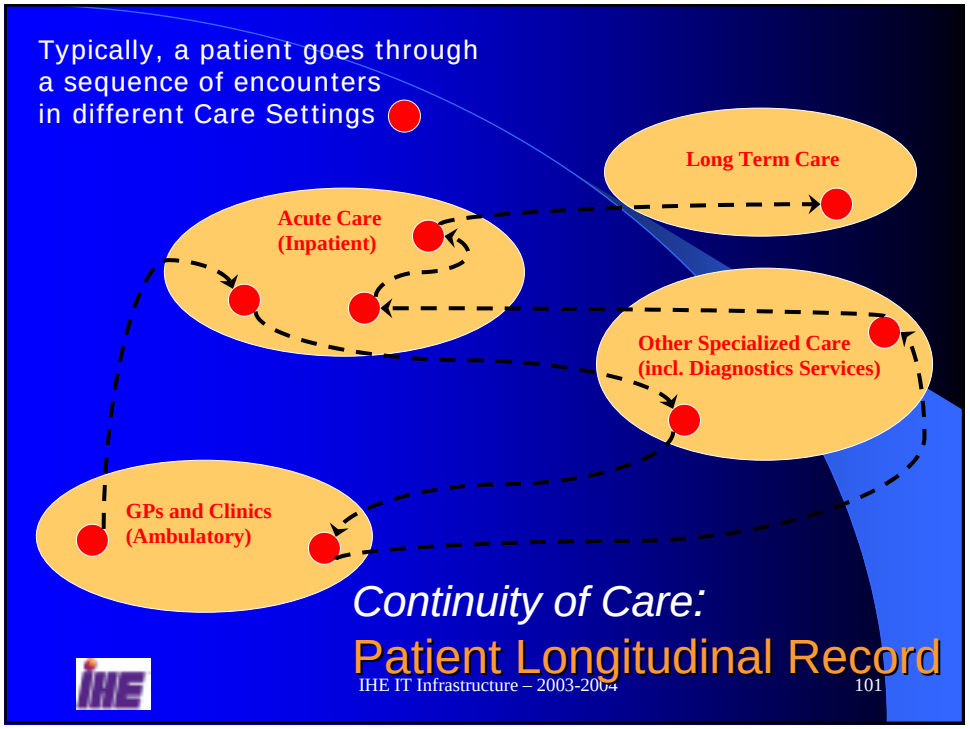
EHR Cross-Enterprise Document Sharing

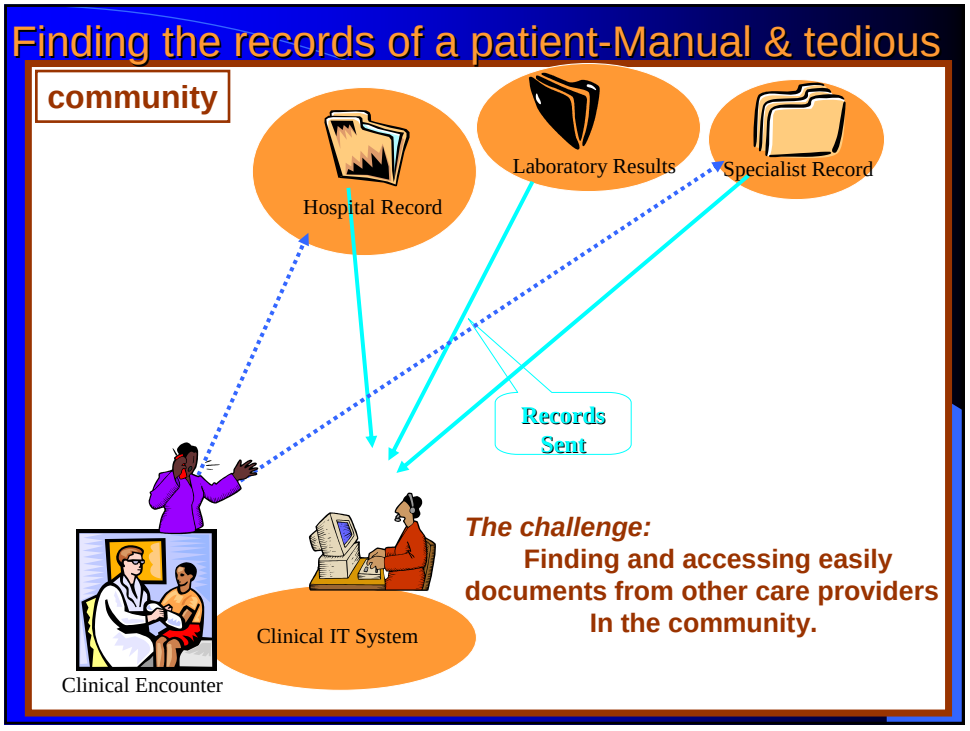
First step towards the longitudinal dimension of the EHR

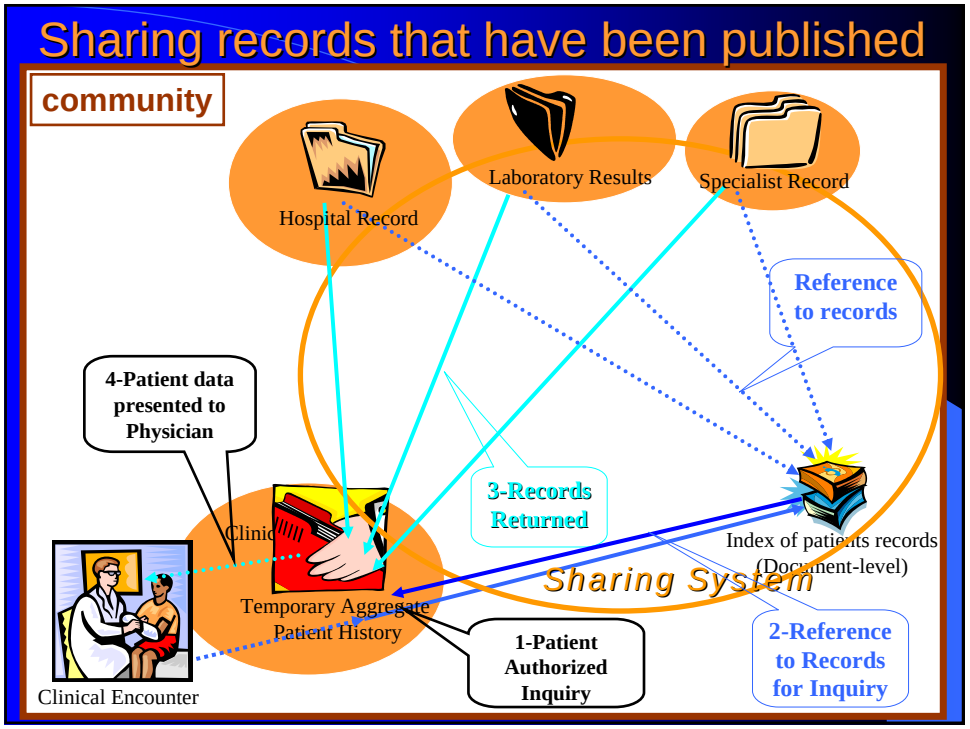
Focus: Support document sharing between EHRs in different care settings and organizations

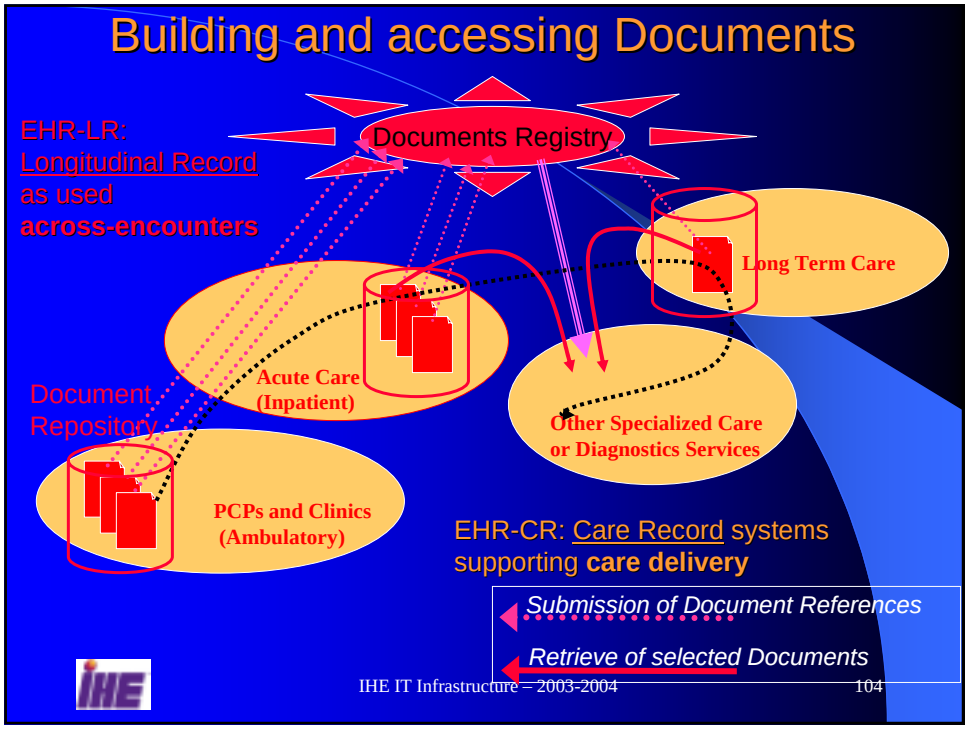
Agenda

- Managing a longitudinal patient record.
- Cross-enterprise Document Sharing (XDS), operations.
- Contribution of documents, organization tools for the physicians
- Using XDS in a cardiac care scenario.
- Choosing the standards for XDS
- Implementation Models
- More technical details


Typically, a patient goes through
a sequence of encounters
in different Care Settings
Long Term Care
Acute Care
(Inpatient)
Other Specialized Care
(incl. Diagnostics Services)
GPs and Clinics
(Ambulatory)
Continuity of Care:
Patient Longitudinal Record


Finding the records of a patient-Manual & tedious
community
Hospital Record
Laboratory Results
Specialist Record
Records
Sent
Clinical IT System
Clinical Encounter
The challenge:
Finding and accessing easily
documents from other care providers
In the community.


Sharing records that have been published
community
Hospital Record
Laboratory Results
Specialist Record
Reference to records
4-Patient data presented to Physician
3-Records Returned
Clinic
Temporary Aggregate Patient History
Index of patients records (Document-level)
Sharing System
1-Patient Authorized Inquiry
2-Reference to Records for Inquiry
Clinical Encounter


Building and accessing Documents
EHR-LR: Longitudinal Record as used across-encounters
Documents Registry
Long Term Care
Acute Care (Inpatient)
Document Repository
Other Specialized Care or Diagnostics Services
PCPs and Clinics (Ambulatory)
EHR-CR: Care Record systems supporting care delivery
Submission of Document References
Retrieve of selected Documents

XDS – Value Proposition

- Foundation for Health IT Infrastructures: Shared Electronic Health Record, in a community, region, etc.
- Effective means to contribute and access clinical documents across health enterprises.
- Scalable sharing of documents between private physicians, clinics, long term care, pharmacy, acute care with different clinical IT systems.
- Easy access: Care providers are offered means to query and retrieve clinical documents of interest.

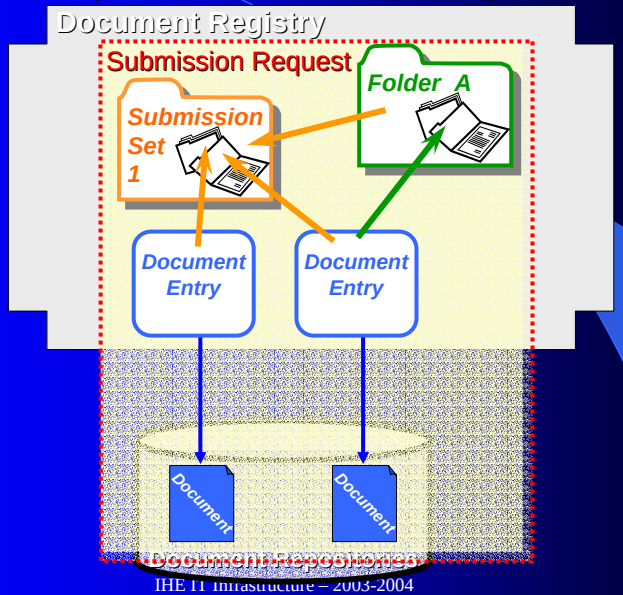
XDS - Value Proposition

- Distributed: Each Care delivery organization "publishes" clinical information for others. Actual documents may remain in the source EHR-CR.
- Cross-Enterprise: A Registry provides an index for published information to authorized care delivery organizations belonging to the same clinical affinity domain (e.g. an LHII).
- Document Centric: Published clinical data is organized into "clinical documents". using agreed standard document types (HL7-CDA, ASTM-CCR, PDF, DICOM, etc.)
- Document Content Neutral: Document content is processed only by source and consumer IT systems.
- Standardized Registry Attributes: Queries based on meaningful attributes ensure deterministic document searches.

IHE XDS Integration Profile: Key Concepts

- **XDS Document**
- **XDS Submission Set**
- **XDS Folder**

Document Repository and Registry
Example of Submission Request



IHE XDS Integration Profile: Key Concepts

XDS Document

- A set of attested clinical information (structured or not) which form an element of a patient record to be shared. It may already exist within the source IT system.

XDS Submission Set

- A set of documents related to a patient that a (team of) clinician(s) in the same source system have decided to make available to potential consumers.

XDS Folder

A means to group documents for a number of other reasons:

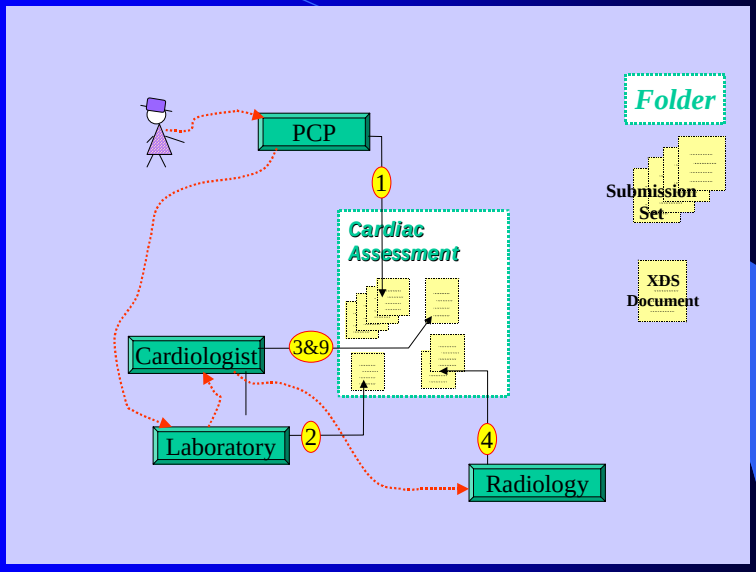
- Team work across several physicians,
- Episode of care,
- Emergency information for a patient, etc.

XDS leaves open the use of folders to affinity domain clinicians.

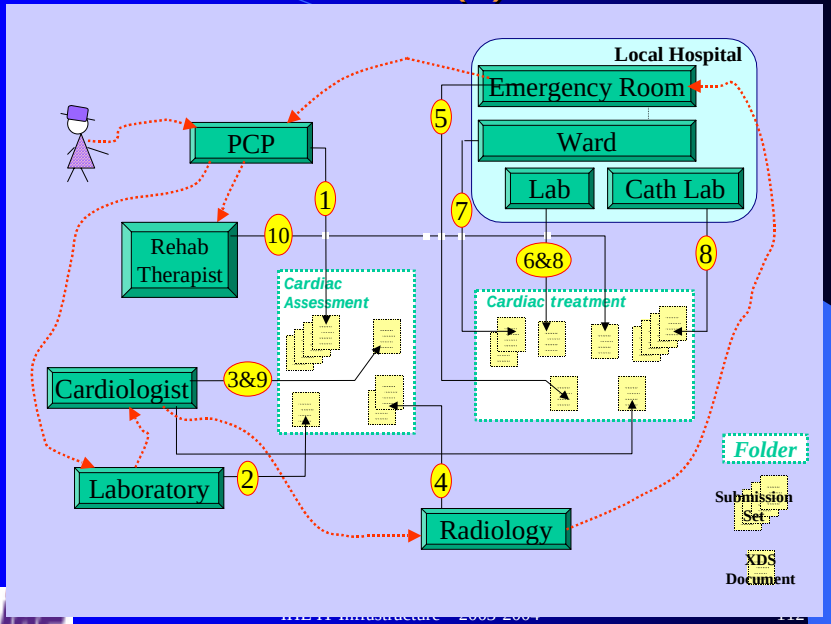
EHR Cross-Enterprise Document Sharing What does IHE deliver ?

- A set of practical scenarios: Submission of documents, submission set, folder, affinity domains, etc are derived from use case scenarios. Example: cardiac care network.
- A definition of the Actors involved: XDS relies on 5 Actors implemented by the IT systems involved.
- A complete specification of the Transactions involved : XDS include 5 Transactions specifying exchange of one or more standards-based messages. XDS leverages the most appropriate standard(s) (e.g. HL7, ebXML, W3C, etc.) and resolves any options to ensure interoperability.
- A number of implementation scenarios are discussed.

Cardiac Care Scenario (1)

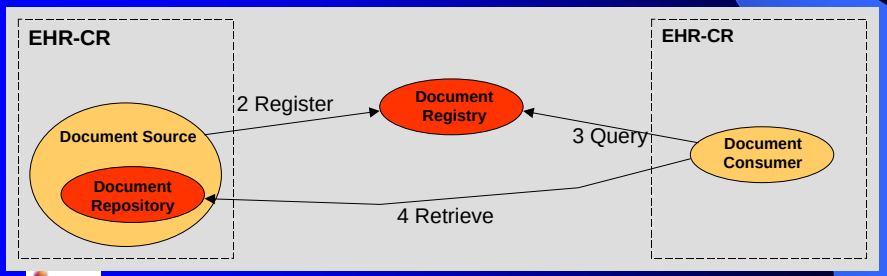


Cardiac Care Scenario (2)



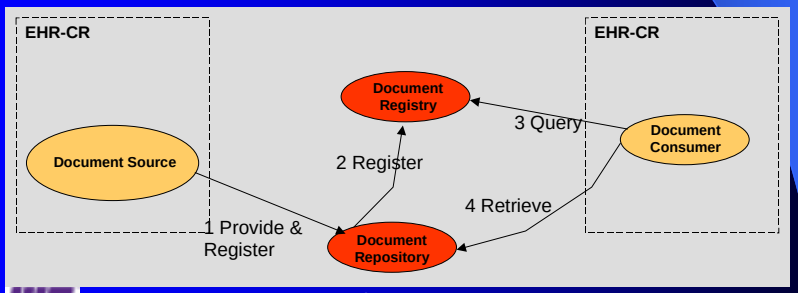
Integration Model 1:
EHR-CR with Repository at Source

- An EHR-CR completes a phase of care for a patient where it:
  - **Has** these documents **available** as Repository Actor.
  - **Registers** documents with a Registry actor.
- Any other EHR-CR may query the Registry actor, and chose to retrieve some of these documents from any Document Repository Actor.



Integration Model 2:
EHR-LR with Third Party Repository

- An EHR-CR completes a phase of care for a patient where it:
  - **Provides** the documents to a Repository Actor of its choice.
  - Documents are **Registered** with a Registry Actor.
- Any other EHR-CR may query the Registry actor, and chose to retrieve some of these documents from any Document Repository Actor.



Integration Model 3:
EHR-CR feed a EHR-CR/EHR-LR hub

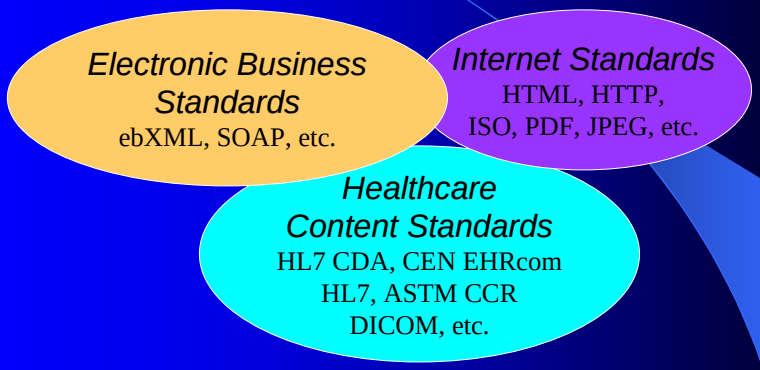
- An EHR-CR completes a phase of care for a patient where it:
  - **Provides** and **Registers** a set of documents to a Document Repository in an EHR-CR.
- The EHR-CR Consumer Actor has the documents and may respond to queries and provide them to other document consumers.

Patient Access also possible

- A patient accesses own record:
  - **Query** and **Retrieve** a set of documents using for example a portal application that offers the ability to display documents' content.
- This is a particular case of an EHR-CR, where the patient is interested her/his own care. Patient may also register and provide documents.

Standards selection for IHE XDS

No single standard can address Cross-enterprise Document Sharing



Marriage of healthcare standards facilitates implementation and leverages complementary technologies (e.g. security & privacy).

Conclusion:

IHE Cross-Enterprise Document Sharing

- *IHE does not claim with XDS to address all aspects of a complete and interoperable EHR System.*
- *Access Control and Doc Content Profiles are on the IHE Roadmap for 2005.*
- In **collaboration** with well established standards bodies (HL7, ASTM, CEN, OASIS, IETF, DICOM, etc.) and other EHR related initiatives world-wide (EuroREC, etc.),
  IHE expects to ***contribute at a more cost-effective and rapid deployment*** of community, regional and national health IT infrastructures.

XDS – Conclusion

- **Foundation for EHR & Health IT Infrastructures**
- **Effective contribution and access to shared documents across all types of health enterprises**
- **Scalable, Flexible and Easy access**

XDS to be one of the major highlights of **2005 Annual HIMSS Conference & Exhibition**. Dallas, Tex., Feb. 13-17:

- used as a foundation for an on-site demonstration of interoperability in support of a National Health Information Networks.
- Attendees at the conference will be able to create and share their own health records across vendor booths as well as in the ambulatory and acute care settings on the conference exhibit floor.

How real is XDS ?

- Specification work since Nov 2003
- Under Public Comments June-July 2004
  - 600 constructive comments received.
  - *Validity of XDS approach confirmed* ***(e.g. CfH Roadmap).***
- Stable specification IHE Technical Framework Published Aug 15th, 2004 (TI Supplement)
- IHE Connectathon - January 2005 (USA)
- *HIMSS Feb 2005 - show-wide demonstration*
- IHE Connectathon - April 2005 (Europe)

Several Implementation Projects by health authorities in 2005

Integrating the Healthcare Enterprise

施設間ドキュメント共有

詳細

Keith W. Boone – Dictaphone Corporation

IHE IT Infrastructure Technical Committee

Agenda

1. **Standards**
2. **Actors and Transactions**
3. **Document**
4. **Submission Set**
5. **Folder**
6. **Submission Request**
7. **Affinity Domain**
8. **Patient Identification**
9. **Document Lifecycle**
10. **Security and Privacy**

Standards for XDS

No single standard addresses XDS Requirements

Healthcare Content Standards

- HL7 Version 2.3.1
  - Messages for Patient Identity Management
- HL7 Version 2.5
  - Datatypes for XDS Registry Attribute values
- HL7 CDA Release 1
  - XDS Document concept definition
  - XDS Document Content
  - Source of XDS Document Entry Attributes
- DICOM, ASTM CCR, HL7 CDA Release 2, CEN EHRcom
  - XDS Document Content
  - Sources of XDS Document Entry Attributes

Internet Standards

- HTTP
  - Protocol for Retrieve Document
  - Online SOAP bindings
- SMTP
  - Offline ebMS bindings
- IETF
  - Language Identifiers
- MIME
  - Document Type codes
- PDF, JPEG, HTML
  - XDS Document Content
- UTF-8
  - Encoding of Registry Attributes

Electronic Business Standards

- OASIS/ebXML
  - Registry Information Model v2.0
    - Basis of XDS Registry Information Model
  - Registry Services Specifications v2.0
    - Registry Services
  - Messaging Services Specifications v2.0
    - Offline protocols
- ISO/IEC 9075 Database Language SQL
  - Registry Query Language
- SOAP with Attachments
  - Protocol for communication with XDS Registries and Repositories

Actors (Application Roles)

Document Source (EHR-CR)

- Healthcare point of service system where care is provided and associated clinical information is first collected

Document Registry (EHR-LR)

- Index and metadata database for all published clinical documents that may be queried.

Document Repository (EHR-LR)

- Maintains and stores published documents that may be retrieved

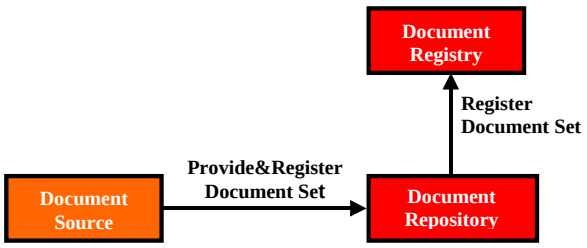
Document Consumer (EHR-CR)

- Healthcare point of service application system where care is provided that needs access to documents and information

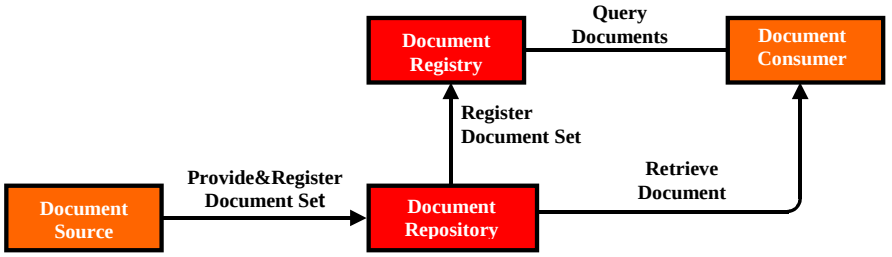
Patient Identity Source (EHR-LR)

- Assigns and managed Patient identifiers for the XDS Sharing Domain

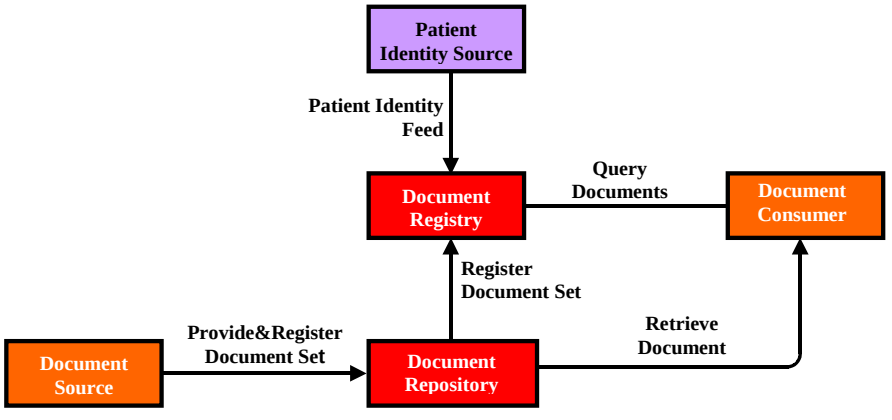
XDS Actors and Transactions



XDS Actors and Transactions



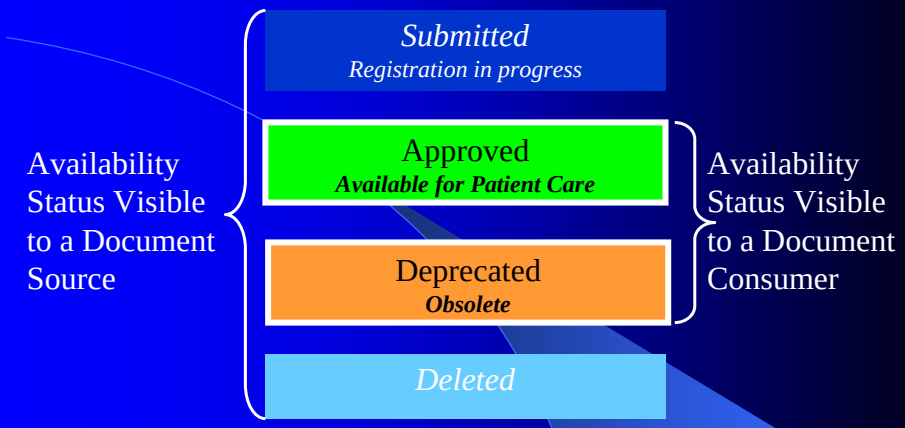
XDS Actors and Transactions



XDS Document

- Is the smallest unit of information provided to a Document Repository and registered in the Document Registry.
- Contains observations and services for the purpose of exchange (See HL7 CDA Release 1).
- Must be human and/or application readable.
- Complies with a published standard.
- Shall be associated with Meta-data defined by the Document Source, managed by the Document Registry, and used for query Document Consumers.
- Shall be provided to the Document Repository as an octet stream associated with a MIME type to be retrieved unchanged.

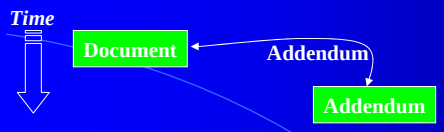
Document Availability Management



Availability Status Change under the Control of Original Document Source and Patient (if allowed in Affinity Domain)

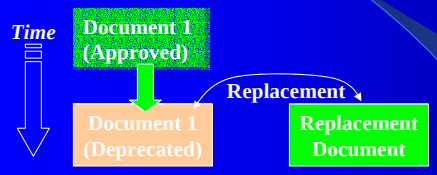
Document Life Cycle Management

Addendum to a registered document



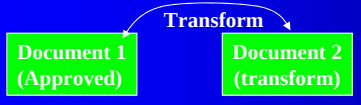
A two-way relationship between Original and Addendum

Replacing a registered document by a new document



A two-way relationship between Original and Replacement Document.

Registering an alternate form of a registered document

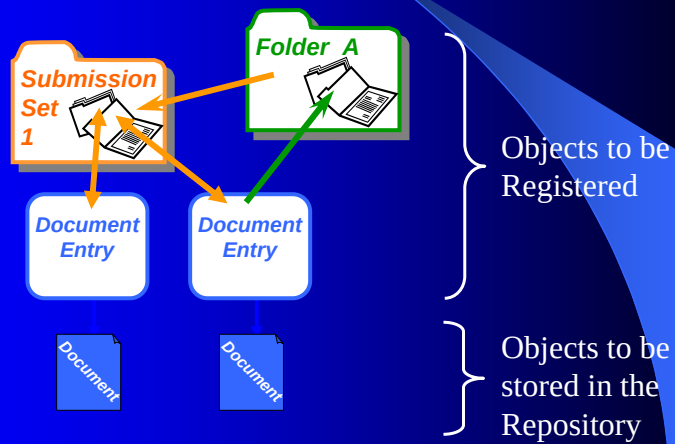


A two-way relationship between Original and Transform (alternative format with same scope).

XDS Submission Set

- Created by a single Document Source.
- Issued by a single Provide & Register Document Set or Register Document Set transaction.
- Related to care event(s) of a uniquely identified patient.
- Records new documents.
- References prior documents.
- Associated with a “content code” (e.g. clinical meaning) by the Document Source.
- Accessible via the Query Registry transaction.

Example:
Document Source prepares a submission request :
*One **Submission Set***
associated with two Documents and a Folder



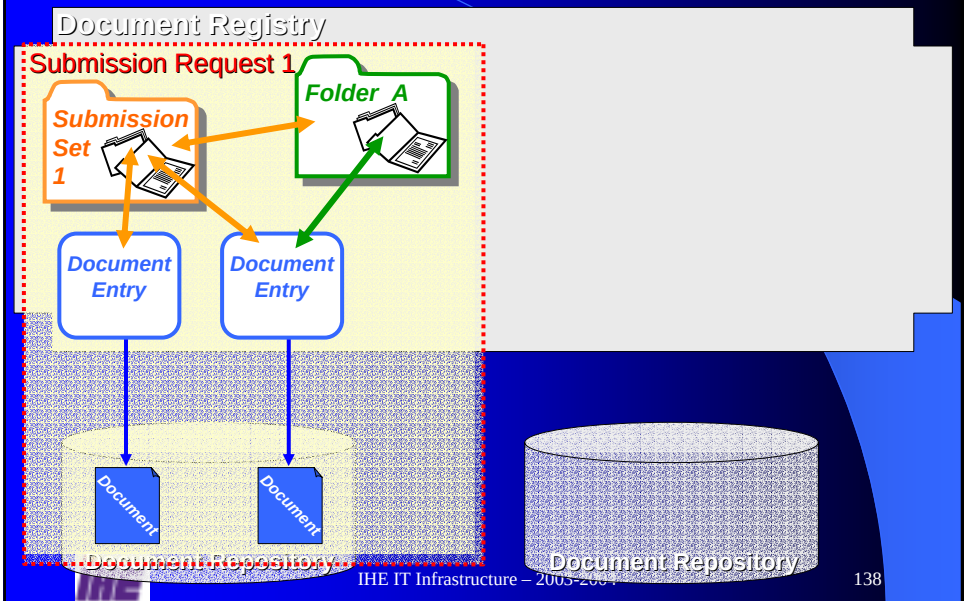
XDS Folder

- A means to group one or more documents for any reason.
- Groups documents related to a single patient.
- May include contributions from one or more Document Sources.
- Can have new or existing documents inserted at anytime by a Document Source.
- Will be permanently known by the registry.
- Accessible via the Query Registry transaction.
- Associated with a code (e.g. clinical meaning) by Document Sources.

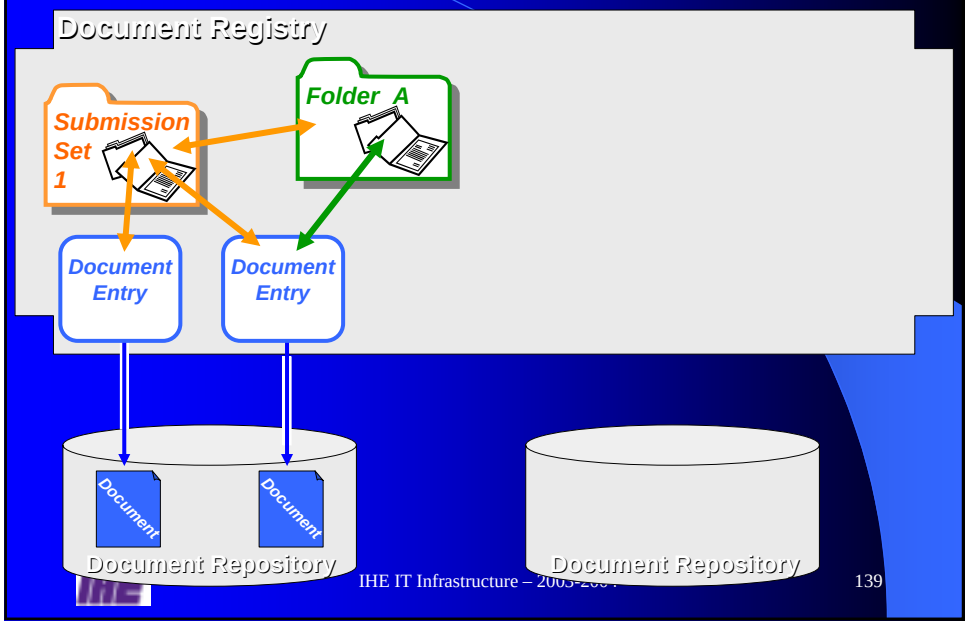
XDS Submission Request

- Created by a Multiple Submission Request or Single Provide & Register Document Set transaction.
- Includes a Submission Set and zero or more:
  - new documents
  - references to existing documents
  - folders
  - associations of documents with folders.
- Registered Atomically in a single transaction.
  - Upon successful submission all of the new objects it creates are available for sharing, otherwise none are.

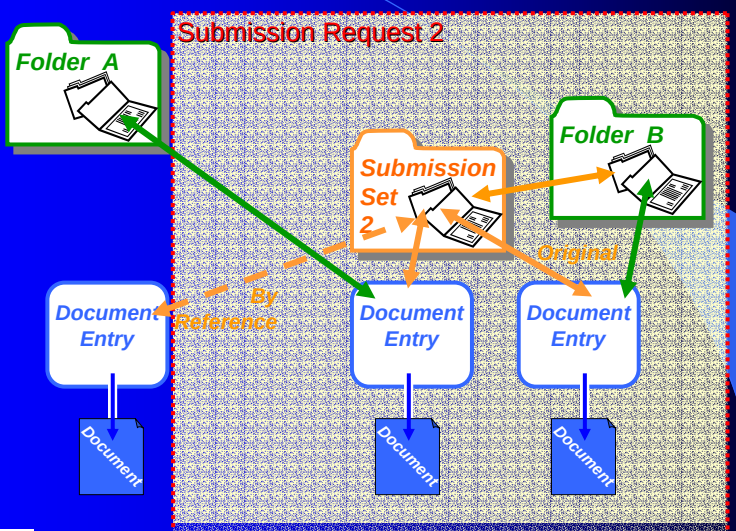
Document Repository and Registry – First Submission



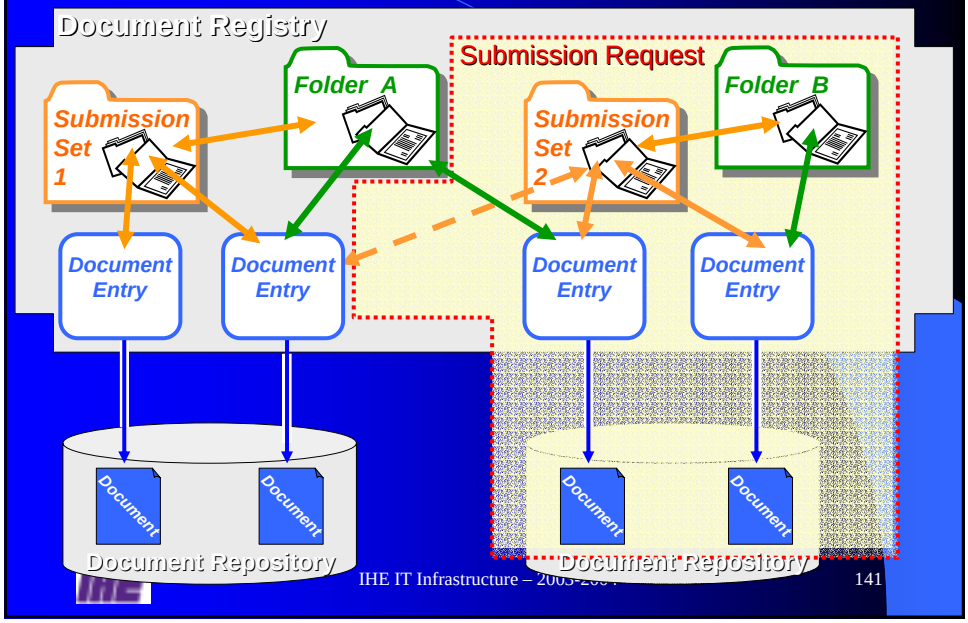
Document Repository and Registry – After Submission Request succeeded



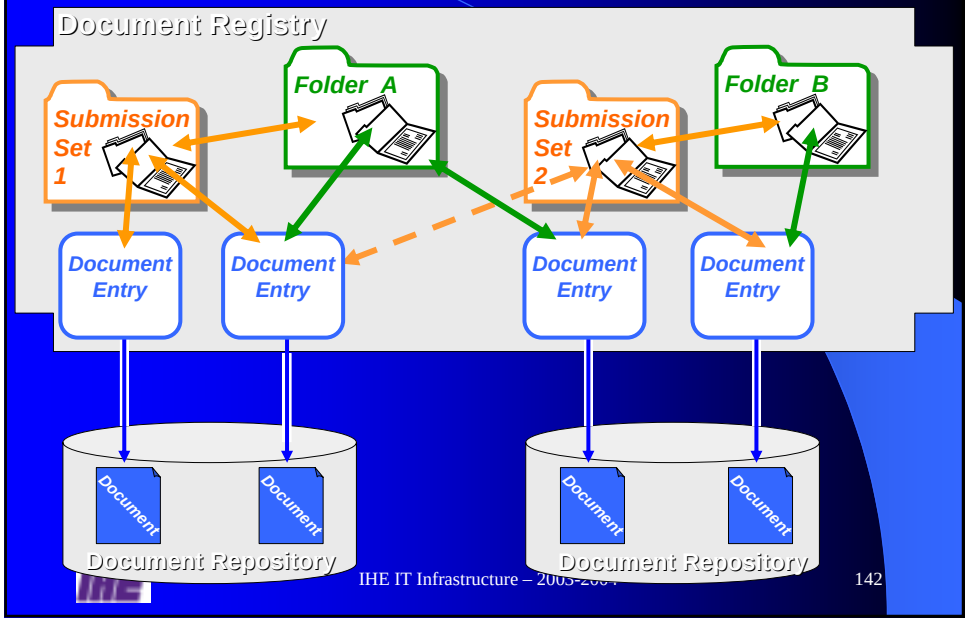
Submission Request 2 - Logical Content



Document Repository and Registry – Submission Request 2



Document Repository and Registry – Final State

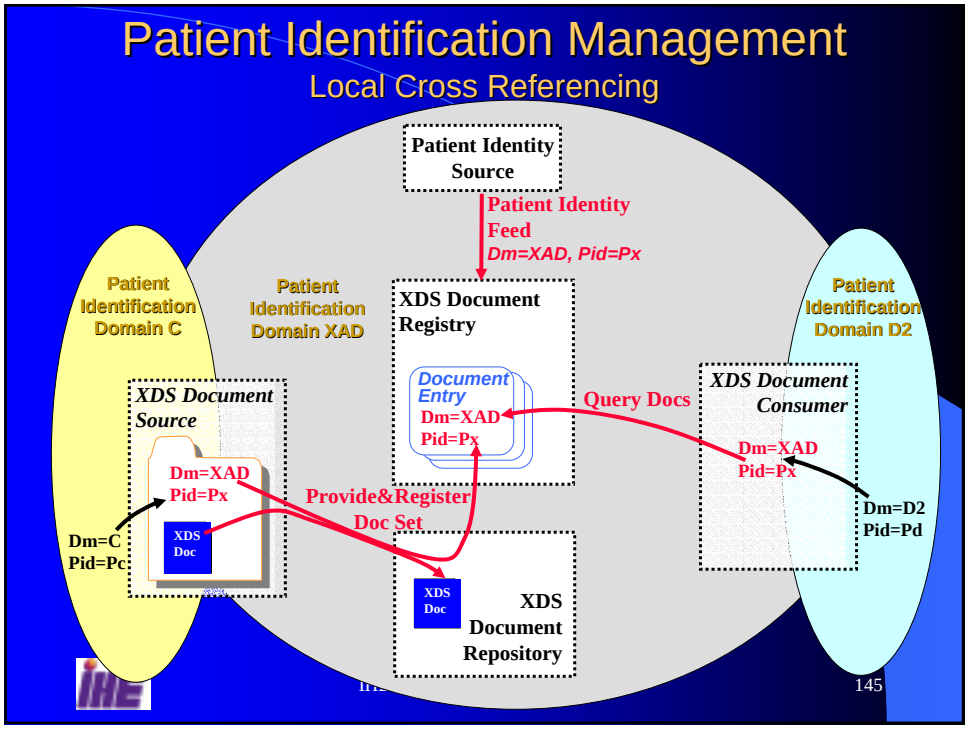


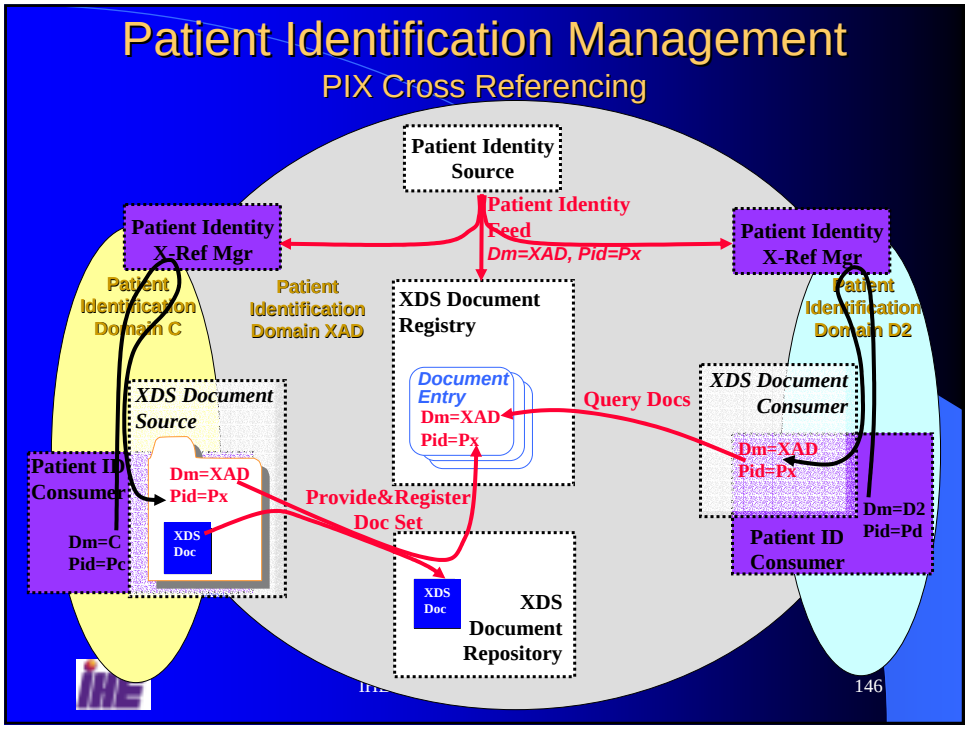
XDS Affinity Domain

- Implements a single Document Registry
- Identifies:
  - Document Sources
  - Document Consumers
  - Document Repositories
- Assigns Patient Identity Domain
- Selects Vocabularies
- Establishes Document Sharing Polices
- Establishes Security and Privacy Policies
  - Is the Source of ATNA node certificates

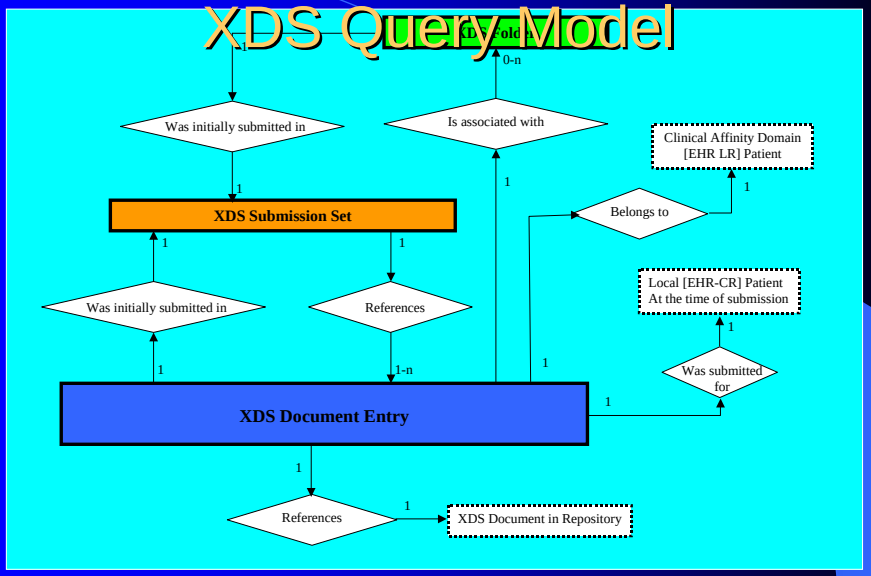
Patient Identification Management

- One Patient Identity Domain
  - Managed by Patient Identity Source.
  - Accessed by Document Registry.
- Multiple methods to map into the Domain
  - Using PIX
  - Using PDQ
  - Other Mechanisms


Patient Identification Management
Local Cross Referencing
Patient Identity Source
Patient Identity Feed
Dm=XAD, Pid=Px
Patient Identification Domain C
Patient Identification Domain XAD
Patient Identification Domain D2
XDS Document Registry
Document Entry
Dm=XAD
Pid=Px
Query Docs
XDS Document Consumer
Dm=XAD
Pid=Px
XDS Document Source
Dm=XAD
Pid=Px
XDS Doc
Provide&Register Doc Set
Dm=C
Pid=Pc
Dm=D2
Pid=Pd
XDS Doc
XDS Document Repository
145

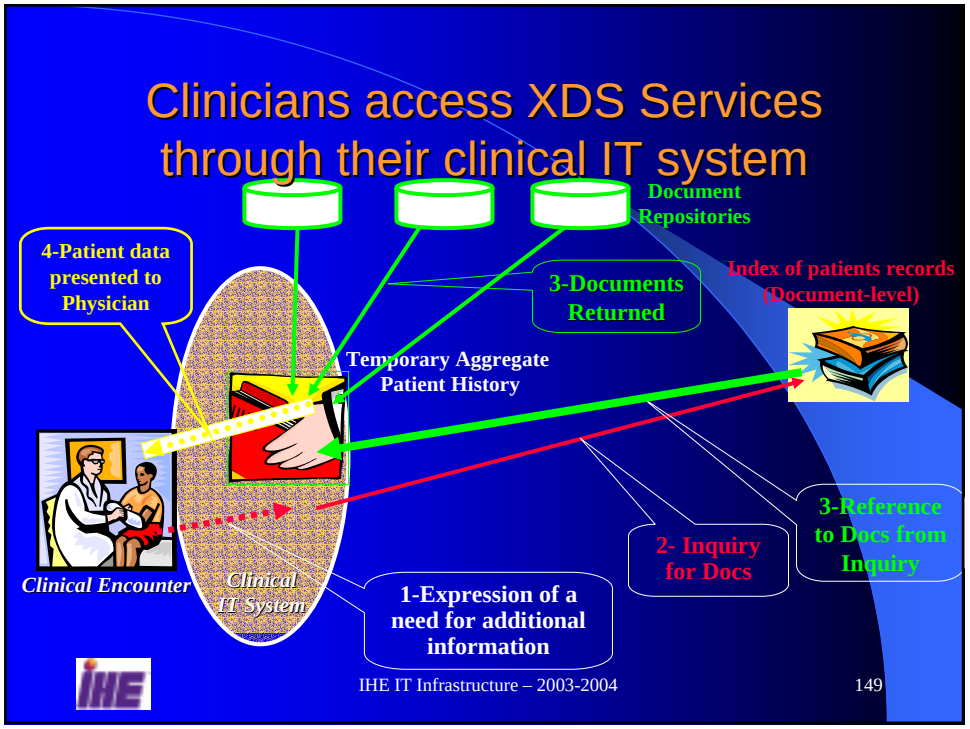

Patient Identification Management
PIX Cross Referencing
Patient Identity Source
Patient Identity Feed
Dm=XAD, Pid=Px
Patient Identity X-Ref Mgr
Patient Identity X-Ref Mgr
Patient Identification Domain C
Patient Identification Domain XAD
Patient Identification Domain D2
XDS Document Registry
Document Entry
Dm=XAD
Pid=Px
Query Docs
XDS Document Consumer
Dm=XAD
Pid=Px
XDS Document Source
Patient ID Consumer
Dm=XAD
Pid=Px
XDS Doc
Provide&Register Doc Set
Dm=C
Pid=Pc
Dm=D2
Pid=Pd
Patient ID Consumer
XDS Doc
XDS Document Repository
146

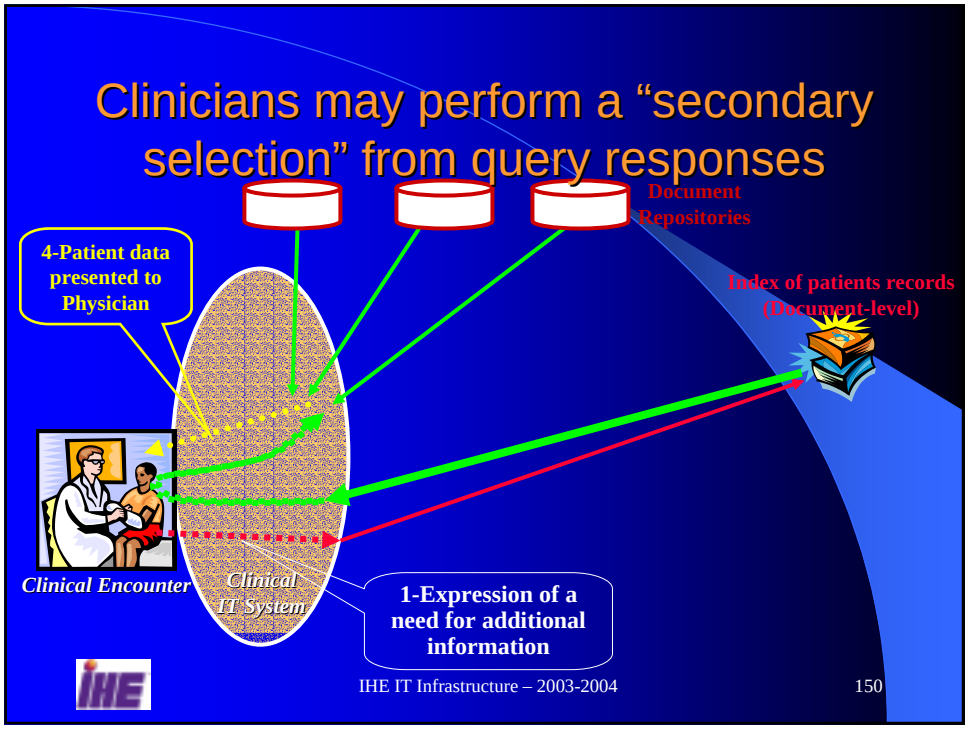
XDS Query Model



XDS Query Principles

- Query Keys: Against a generic set of "document attributes" to ensure deterministic searches, e.g.:
  - Patient Id
  - Service Start and Stop Time
  - Document Creation Time
  - Document Class Code and Display Name
  - Practice Setting Code and Display Name
  - Healthcare Facility Type Code and Display Name
  - Availability Status (Available, Deprecated)
  - Document Unique Id
- Query Keys: Against a generic set of submission set/Folder attributes to ensure deterministic searches, e.g.:
  - Submission Set Id and Content Code.
  - Submission date/time
  - Folder Id and List of Content Codes
  - Folder last update date/time


Clinicians access XDS Services through their clinical IT system
Document Repositories
4-Patient data presented to Physician
3-Documents Returned
Index of patients records (Document-level)
Temporary Aggregate Patient History
3-Reference to Docs from Inquiry
2- Inquiry for Docs
Clinical Encounter
Clinical IT System
1-Expression of a need for additional information
IHE IT Infrastructure – 2003-2004
149

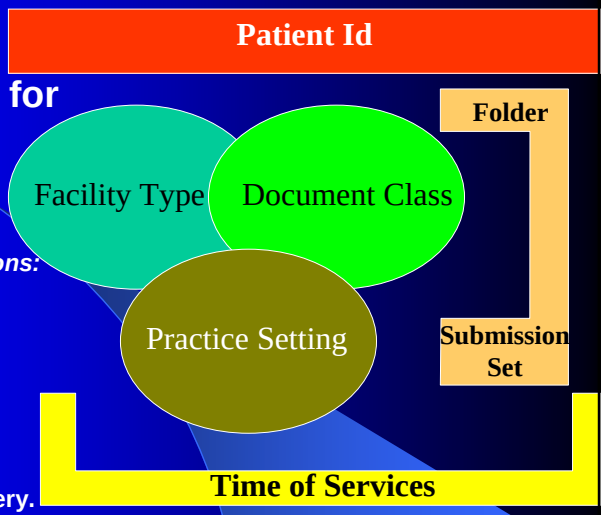

Clinicians may perform a “secondary selection” from query responses
Document Repositories
4-Patient data presented to Physician
Index of patients records (Document-level)
Clinical Encounter
Clinical IT System
1-Expression of a need for additional information
IHE IT Infrastructure – 2003-2004
150

Querying for Documents

The four main axes for Document Queries:

1. Which Patient ?
2. What Type of Document ?
   - ***3 interrelated sub-dimensions:***
   - *Facility Type*
   - *Document Class*
   - *Event Type*
3. By Groups of Documents
4. By time of Services

10 additional attributes to query.



XDS core Meta-Data derived from HL7 CDA and CEN EHRcom

Security for XDS

Leverages IHE Audit Trail & Node Authentication

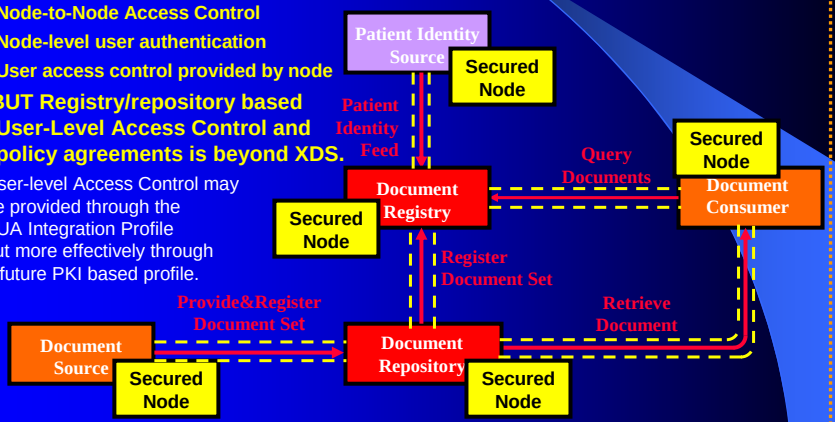
A formal Security and Privacy profile is provided for XDS

ATNA creates a secured domain:

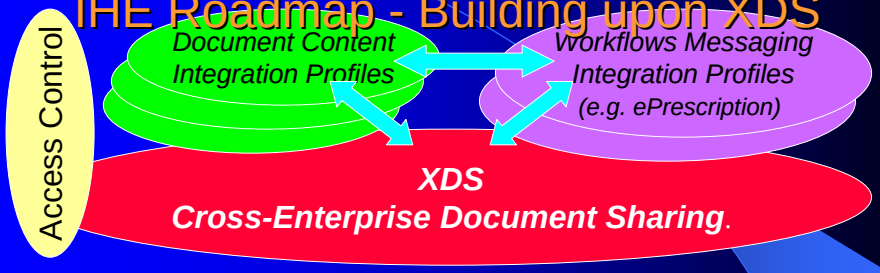
- User Accountability (Audit trail)
- Node-to-Node Access Control
- Node-level user authentication
- User access control provided by node

BUT Registry/repository based User-Level Access Control and policy agreements is beyond XDS.

User-level Access Control may be provided through the EUA Integration Profile but more effectively through a future PKI based profile.



IHE Roadmap - Building upon XDS



XDS is a foundation building block for cross-enterprise EHR:

- **Document Content Integration Profiles** will define for a specific domain of care practice: document format, content vocabularies, templates, etc.).
- **Workflow messaging Integration Profiles** will define messages to support specific workflows (ePrescribing, eReferral, eBooking, etc.). These messages should simply reference XDS managed documents for persistent artifacts.

Questions?

More information….

- IHE Web sites:
  - http://www.himss.org/IHE
  - http://www.rsna.org/IHE
  - http://www.acc.org/quality/ihe.htm
- Technical Frameworks:
  - **ITI V1.0, RAD V5.5, LAB V1.0**
- Technical Framework Supplements - Trial Implementation
  - **May 2004: Radiology**
  - **August 2004: Cardiology, IT Infrastructure**
- Non-Technical Brochures:
  - **Calls for Participation**
  - **IHE Fact Sheet and FAQ**
  - **IHE Integration Profiles: Guidelines for Buyers**
  - **IHE Connect-a-thon Results**

Conclusion

XDS automates an existing manual process, utilizing multiple standards, to enable the creation of a longitudinal record, giving providers easier access to clinical data, and thereby providing for better overall patient care.

IHE ITインフラをどのように進めるか

1. **Read IHE Fact Sheet & this presentation**
   - www.himss.org/ihe
2. **Read ITI *Technical Framework Vol 1*** Integration Profiles
   - www.himss.org/ihe
3. **Read ITI *Technical Framework Vol 2*** Transactions
   - www.himss.org/ihe
4. ***IHE IT Infrastructure Tech. Committee* has issued the final text for technical framework version 1.0 in June 2004.**
5. **Final IT Infrastructure Technical Framework V1.0 includes the feedback from HIMSS HL7-IHE and IHE-Europe Connectathons.**