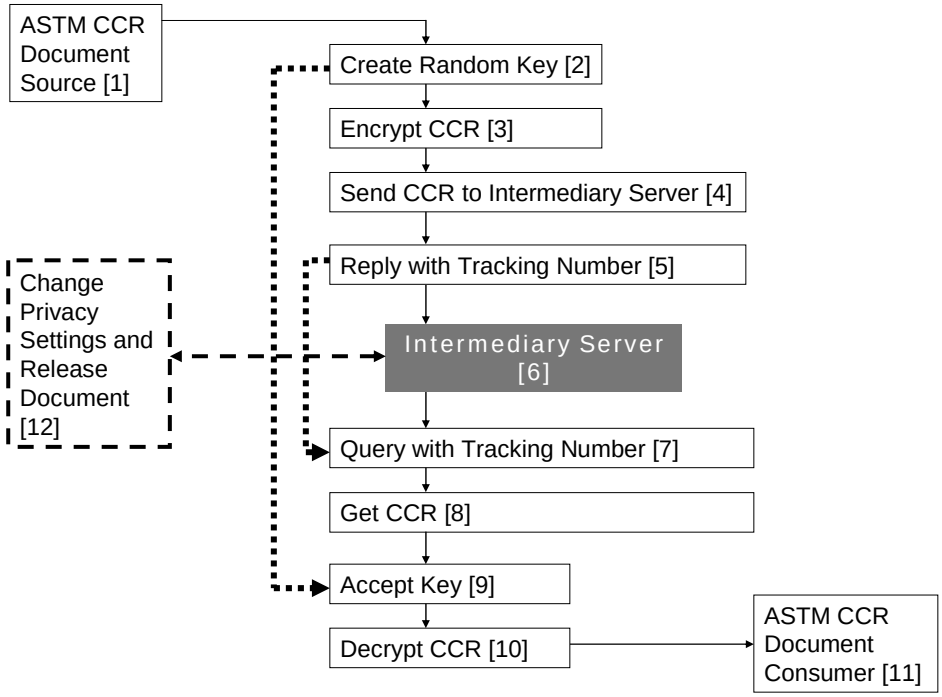
METHOD FOR EXTENDING AN INFORMATION STANDARD THROUGH COMPATIBLE ONLINE ACCESS

Illustrated by Application to Patient Privacy and the CCR

Adrian Gropper MD
MedCommons
August 16, 2005 (v1 – 7/16/05)



Brief Description:

In the standards-based transport path from Document Source [1] to Document Consumer [11] {thin solid arrows}, an Intermediary Server [6] intercedes on behalf of the User or the Patient [12] to implement their privacy mandates even when the standards-based systems {thin frames} do not or cannot implement advanced privacy features. Standards-based document encryption means [2, 3] and document decryption means [9, 10] perform routing and key exchange based on simple identity (Tracking Number) [5, 7] and security (Key) [2, 9] as if they were executing a simple point-to-point transfer backed by identity and key transfers {heavy dotted arrows}, each one connecting to the Intermediary Server [6] as its standards-based peer and unaware that a User or Patient [12] with implicit or explicit access to the identity and security keys can manipulate {heavy dashed line and frame} the on-line document contents, its routing and various other privacy-related characteristics that may not be supported by the standard or by their particular source or consumer implementation.

1. Background

Health care is a $1.7 Trillion industry in the US and it is very information intensive. Histories, diagnostics, imaging, treatment plans, disease management, decision support, clinical trials, pay-for-performance, and insurance claims are all examples of information about a specific person as they move through the health care industry. With few exceptions, the patient's control their own movement as they go from one provider to another but they control almost none of their information. Yet, detailed digital information about specific patients: their MRI and CT scans, genetic profiles, family histories, and neuropsychological tests, will impact their entire lives and possibly the lives of their children in ways that can not be foreseen at the time the test is performed.

As new technology makes the digital description of the patient increasingly more authoritative than their physical exam, patients can benefit from being able to offer their digital selves to get sharper diagnoses, better second-opinions, more diverse treatment plans and more effective and less invasive therapies.

Contemporary healthcare information technology seems to be intentionally designed to prevent the direct control of information by the patient. This is hardly surprising for an information technology industry that has evolved almost entirely in a managed care and third-party paid environment where neither patients nor primary care physicians are in a position to buy information technology services. The high value of individual privacy and the patient control of information that underlies effective privacy is going to become increasingly obvious to health care consumers be they healthy or not.

MedCommons has worked to develop the technology for effective patient data banking and communications that are patient centric, patient-accessible, free or very low cost to primary care physicians and independent of both the patient's managed care providers and their insurers. We continue to be surprised by how few institutions are advocating for the patient's privacy interest and have come to feel that MedCommons may be one of the few enterprises founded primarily to profit by effectively protecting the patient's privacy while facilitating their ability to get advice and treatment from the physicians of their choice.

Taken to its ultimate conclusion, MedCommons will allow national-scale patient and physician pools to self-insure for routine and primary care and interact with hospitals, specialized facilities and catastrophic coverage insurers from a position of strength.

2. Introduction

This paper describes a range of privacy innovations embodied in MedCommons as a "privacy services provider". Features of MedCommons that do not have a primary relationship to privacy are not discussed. This paper is intended to serve as a patent disclosure prior to becoming a White Paper regarding the MedCommons service.

MedCommons translates privacy into 21 technical features. These features combine to enable simple and effective control by the patient and by the primary care physician on their patient's behalf. These features are divided into three separate categories:

- Voluntary participation avoids direct or indirect lock-in of the client into MedCommons or any other institution. The ability to "take your business elsewhere" at any time becomes part of the basis of trust in MedCommons as the patient's privacy agent, un-conflicted by treatment or employment relationships.
- Transparency enables the client to see and understand as much of their private information as they care-to, thereby making for truly effective control and real informed consent.
- Comfort and self-respect features attempt to avoid openly questioning a doctor's competence or an institution's policies and protect the client from uncomfortable exposure of private information to administrative and technical support personnel.

3. Voluntary Participation Features

1. Voluntary, non-biometric patient or physician account identifier. Voluntary participation is the most fundamental requirement for preserving the patient's interest. If an institution's policies or actions displease the client, they are free to take their business elsewhere with a minimum of disruption. This is a much better way to assure the protection of the client's interest than legal or bureaucratic processes which have a high activation threshold and an uncertain outcome. Bank accounts and credit card numbers are a familiar example of voluntary identifiers. A social security number, hospital or insurance ID are examples of involuntary identifiers because an attempt to change them usually involves a great deal of work and may impose direct or indirect penalties. Biometric identifiers are even worse because, like a tattoo or cattle brand, they take all control away from the subject.
2. Keep the client's on-site copy in the clear. The client's copy might be the only copy. A client should not be forced to deal with their privacy services provider when they don't need to or can't afford it. Ideally, the client should have a personal copy of all information in their home ready to be disconnected from the privacy service provider at any time without prior notice to the service provider. This local copy can be physically secured or password protected. MedCommons offers an automatic synchronization service that manages a copy of a client account on a flash memory stick or disk drive attached securely and directly to the client's Internet connection.
3. Standards-based. The information in the client's account should not be in any vendor's proprietary format to avoid secondary lock-in or hidden expenses when the client wishes to switch service to a competitor service. MedCommons uses

the ASTM-standard Continuity of Care Record (CCR), open standard PDF for documents and open standard DICOM for imaging as well as Internet standard email and security protocols for notification and authorization.

4. Independent. Any privacy services provider should be independent of healthcare providers, insurers or client employers to avoid conflict of interest.

4. Transparency Features

5. Consent mechanism (implied and informed). Informed consent by the patient is an obvious necessity for maintaining privacy in the face of limited understanding and uncertain circumstances. Although opt-in by informed consent is preferable, safety and expediency often require the patient to grant an implied consent to providers directly involved in their care. The MedCommons service provides both opt-in and implied consent mechanisms and makes the opt-in alternative as easy to use as possible for both patient and physician in order to limit the use of the implied consent as much as possible.
6. Avoid Role Based Access Control. Roles are difficult for patients to understand and for institutions to enforce. Role based access control is hardly transparent to a patient or physician who is unable to review and understand the diverse policies of different institutions. Clear opt-in and informed consent in MedCommons minimize the need for a client to trust in an institution's definition of role.
7. Control of content (while preserving document integrity and authenticity of the original creator's signatures). Physicians are liable for some of the medical information that passes through a patient's account. MedCommons enables the creator and the patient to review every document before passing it on to a destination. If the document is signed by its creator and the client does not alter it, MedCommons preserves the original signature. Encrypted content is also allowed in cases where a provider explicitly wants to prevent a patient from seeing potentially harmful information such as a psychiatric note. Even though the patient cannot see the content, they still have control over whether it is sent on to a destination or not.
8. Editorial control. The patient can review and edit or delete any item that they feel is inaccurate or unnecessary before sending a document on. Edits and deletions obviously invalidate a document's original creator's signature.
9. Open Source. When clients are asked to install software in support of MedCommons services on their computer or local area network (e.g.: to upload PDF or DICOM images or to synchronize a local copy of their documents) MedCommons supplies that software as peer-reviewable open source software to reduce the risk of software vendor lock in and to reduce security risks.

10. No Master Patient Index (MPI). Some cross-enterprise interoperability services attempt to match the identity of patients across different enterprises using MPI databases instead of explicit voluntary identifiers. These systems deduce a patient's identity based on a correlation of multiple and often vague criteria. This approach to controlling access to private documents is circumstantial and quite opaque to the patient who has little idea of what specific information any particular querying institution will turn up depending on what patient characteristics they supply with the query. MedCommons does not operate a MPI and requires that institutional patient identifiers be clearly listed on a consent form before transfer of private information.

5. Comfort and Self Respect Features

11. Do not allow account sharing. It's tempting for a patient to want to share access to his or her account documents with a trusted practitioner. Unfortunately, this places the patient who wants to get multiple second opinions or restrict access to psychiatric or infectious disease history in the position of denying or doubting a provider. MedCommons avoids this embarrassment by a design which makes account sharing impractical while making it almost seamless to transfer a comprehensive subset of information to a primary care practitioner or consultant.
12. Parallel storage and notification. It's embarrassing and potentially unreliable to ask providers to share the information they transfer among themselves. MedCommons design avoids this by automatically making a copy into the patient's account and even allowing the patient to be notified as new information moves among provider institutions.
13. Privacy Score Assignment. Patients and their document sources can use the MedCommons interface to assign a privacy level to their documents. This ranges from low for consent forms and de-identified (anonymous) records to high for genetic profile, infectious disease and neuropsychological information. Allergies, names of health care providers and most medications would typically have a medium low rating and could be readily be made available in emergency situations, while imaging scans and lab results typically score a medium high rating.
14. Filter Desktop according to Privacy Score and Age. MedCommons provides easy to use tools for a patient to restrict transfer of information to a provider, regional medical data registry or institution based on the Privacy Score and age of each document. As a patient's account accumulates diverse and complex documents, this capability makes it easier for a client to create a subset that is appropriate for a specific situation without automatically defaulting to "send everything".

15. Restrict support and / or emergency access by Privacy Score. Patients requiring technical or clerical support from their privacy services provider should not have to expose their private information. The MedCommons Privacy Score makes it clear that our support and administrative personnel will not see any information above the lowest Consent and De-identified levels. Demo data sets are available for temporary inclusion in a client account to facilitate technical support of viewer and editor functions.

16. MedCommons provides a CCR Send tool that accepts unencrypted CCRs, encrypts them with a user-selectable PIN and sends the CCR to the destination by way of a (temporary or voluntary) MedCommons account – returning a Tracking Number (which is also emailed or faxed to the patient and destination). Anyone with the CCR Tracking Number and PIN can see the contents online. Anyone with the Tracking Number alone can get a copy of the ASTM-standard encrypted CCR. MedCommons assigns a Privacy Score of PS 4 to CCRs (and their attached references) by default to indicate that MedCommons does not have the PIN or access to the encrypted contents ***and forwards the encrypted CCR to its destination.*** A user with the PIN can selectively allow MedCommons to manage access (to a CCR, CCR component or a reference) by selectively removing that PIN and replacing it with one that MedCommons knows or by simply sending the PIN to MedCommons. This activity reduces the Privacy Score accordingly.

17. CCRs are shown as Folders in MedCommons. A Folder has a Privacy Score that can be manipulated by the account holder (patient)

    PS 4 all contents encrypted per ASTM CCR and MedCommons does not have the key. ***This is the CCR Tool Default.***

    PS 3 some contents encrypted with a key that MedCommons has. This content is visible to the user. This is a MedCommons UI feature to be implemented in future versions either client and/or server-side.

    PS 2 all content is visible to the user and MedCommons has the key. ***This is what happens when a user opens a Tracking Number online and gives MedCommons a PIN.***

    PS 1 content is available to emergency personnel and MedCommons support based on role. This is a dropdown on the Desktop and CCR Tab UI.

    PS 0 Demonstration content is anonymous and can be seen by anyone. This is a dropdown on the Desktop and CCR Tab UI.

18. Privacy Scores can be manipulated via the MedCommons user interface but may not be transmitted along with the CCR except to the extent that ASTM CCR spec allows. Therefore,

    A Encrypted CCRs enter a user account as PS 4 because selective encryption (PS 3) is not supported by the standard yet.

    B Unencrypted CCRs enter a user account as PS 2 by default and stay that way until they either expire after a month or are moved to a paid voluntary account.

    C PS 0 and 1 content can be transferred as such between MedCommons accounts. Once they pass out of MedCommons, this convenience distinction is lost because it is not currently supported by the standard.

19. Voluntary account holders can increase the Privacy Score above PS 2 by (selectively) removing control of the encryption key from MedCommons. Until the standard changes, PS 3 may be supported only across MedCommons accounts. PS 4 (ASTM standard encryption) can be applied centrally by MedCommons or using a MedCommons supplied open source client (future). A variant of this technique may be implemented to selectively decrypt parts of a CCR after it's sent by using a Send CCR client that encrypts sections with different keys so that keys can be selectively disclosed to MedCommons. This optimization avoids a content round-trip to the client without requiring the client to trust MedCommons with the key.

20. MedCommons will deliver an ASTM standard encrypted CCR to any destination that supplies a Tracking Number. A client destination that installs the open source Get CCR utility can register with MedCommons to receive unencrypted CCRs onto the client machine. These CCRs are transferred encrypted over the Internet and decrypted locally. The Get CCR utility allows a user to enter a key or PIN for decryption of both standards-based and MedCommons-proprietary PS 3 encryption that is not yet part of the standard.

21. MedCommons eliminates single-point-of failure and service lock-in by supporting local storage tokens for patients and disk drives for practitioners. Local storage is a variation of the Get CCR utility that preserves some of the online MedCommons desktop organization while avoiding proprietary features that would introduce lock-in and reduce archival value. The storage version of Get CCR is also open source software. A user can choose to decrypt their local copy of the Desktop as it's received and 4-dated or leave it encrypted with their master account password. The Master Account Password is assigned by MedCommons to each user when they open a voluntary (paid) account and is sent to the user via US Mail. This allows MedCommons to send to a destination an encrypted copy of their Desktop and associated files at any time without further user authentication.

6. Glossary

- Privacy Services Provider – An agent that provides document transfer and archival storage services to their clients.
- Client – An individual person, including both patients and physicians, with a privacy interest. The patient interest is to control access to personal information much as they would control access to their blood. The physician's privacy interest stems from legal conformance requirements and a desire to avoid control by or lock in to a particular institution. The client is very young or very old they might allow a proxy to control their account.
- Role – Many systems attempt to control access to patient information on the basis of the requester's role [ref a]. Roles are usually defined by an institution or by state or federal law. Roles are often inconsistent across multiple institution and legal jurisdictions.
- ASTM International – One of the oldest and largest standards organization in the world.
- DICOM – A worldwide standard for transmission and storage of medical images.
- PDF – Portable Document Format is an open standard for electronic description of documents as they would print.
- CCR – Continuity of Care Record – An ASTM standard designed to summarize the information about patient at a point in time. The CCR is a standardized and comprehensive version of the "patient summary" typically at the center of most electronic medical record software.
- MPI – Master Patient Index – Attempts to correlate information describing a patient across multiple institutions. When it works as designed, an MPI can make frustrate a patient's attempts to control their information by using different names under different situations.
- Registry – A currently fashionable architecture that "registers" (indexes) documents that can remain stored in their original location. The broader a registry's coverage, the more difficult it is to develop practical policies for access to the registry's information.
- Master Account Password (MAP) – A key that is mailed to a user and encrypts the associated MedCommons account Desktop. This combination of MAP and Postal Address is the default authentication mechanism in MedCommons and part of our password reset-process when users lose access to their account.

7. Bibliography

- NHS (Great Britain) Connecting for Health Privacy Guidelines

8. Draft Claims

Claim 1 might be:

1. MedCommons Send CCR encrypts (per the ASTM standard whatever it is or becomes) using a key PIN that MedCommons may or may not have. This encryption is the default. A Tracking Number or other means of identifying the CCR is returned to the user.
2. MedCommons returns the encrypted CCR to anyone (via CXP or other trivial, irrelevant and insecure protocol). The combination of 1 and 2 establishes the standards-based aspect of our transport business model. Routing and Notification can happen around the standard without any on-line access by anyone and without any proprietary barriers by MedCommons. MedCommons can offer this for free if we choose.
3. Anyone can access MedCommons online and supply the PIN to manipulate the privacy aspects of the transfer as well as the routing.This is the proprietary piece. In the disclosure paper I cal this the Privacy Score. This combination of 1, 2 and 3 is simple, fundamental and should be a very strong patent that does not mess with the standard or the ability to provide competitve banks of medical information that do not offer the online privacy manipulation feature of MedCommons.

Claim 2 adds to Claim 1:

1. A Get CCR client software utility that takes the standards encrypted CCRs (that anyone can get and use if they have the PIN) and adds non-standard or pre-standard privacy features such as the ability to control the encryption of separate sections or attached documents before delivering an un-encrypted CCR to the local user's electronic health record system software. This utility will be delivered as open source software and covered by this Claim 2 even when embedded in the EHR software. This too does not conflict with a standard because Claim 1 does not appy to standards-based encryption that is not modified by an on-line intermediary.

Claim 3 adds to Claim 1:

1. A master account password (MAP) that is sent by mail to all users who register with MedCommons. This key controls the proprietary features of the user's account - including the privacy features in Claim 1 and 2 and others that are described in the document. The combination of a MAP and postal address allows users control over their identity without involving MedCommons primarily in the authentication process. This MAP feature covers major proprietary features of the MedCommons business such as local storage appliances and account termination (Dear John DVD) in the mail that significantly reduce our cost of operating a standards-based and open-source friendly private information bank.

Claim 4 adds to Claim 1:

1. A consent form executed by the user (patient) that directs the on-line transfer agent to route and notify and index and modify information in the (XML) standard document in ways that extend the standard and /or effect the user's preference.

Claim 5 adds to Claim 1:

1. A link between an online service and the online transfer agent of Claim 1 that enables the sending user to enhance an order (request) placed with the online service with information in a standardized medical summary record (CCR) and facilitates the integration of the service's report into an updated CCR.

Claim 6 adds to Claim 1:

1. A user-accessible on-line folder for incomplete or unvalidated medical summary records that require user intervention poor to transfer or permanent storage.

Claim 7 adds to Claim 1:

1. A display of privacy score versus date on the on-line account representation that enhances the ability to sort, merge and maintain an accurate on-live medical summary document (CCR) or multiple separate ones for separate purposes.

Claim 8 adds to Claim 6:

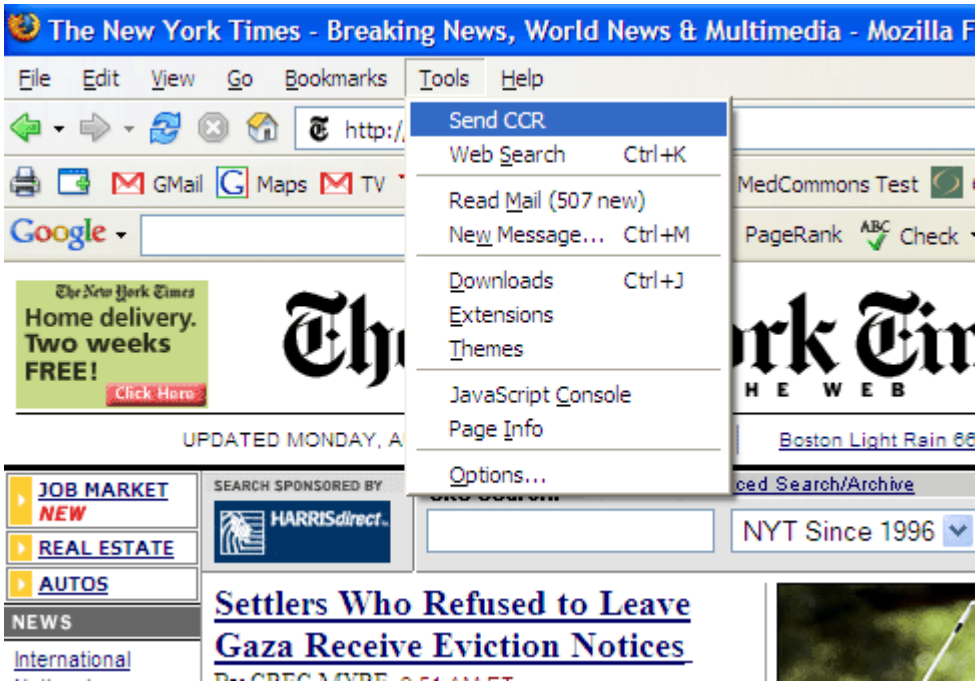
1. A character recognition or format transformation process that requires user intervention or confirmation prior to standards conformance or automated transfer.

Other Names:

- Medical Summary Record Transfer and Storage Agent
- Standards Based On-line Medical Record Transfer Agent
- Standards Enhanced Medical Records Banking Agent

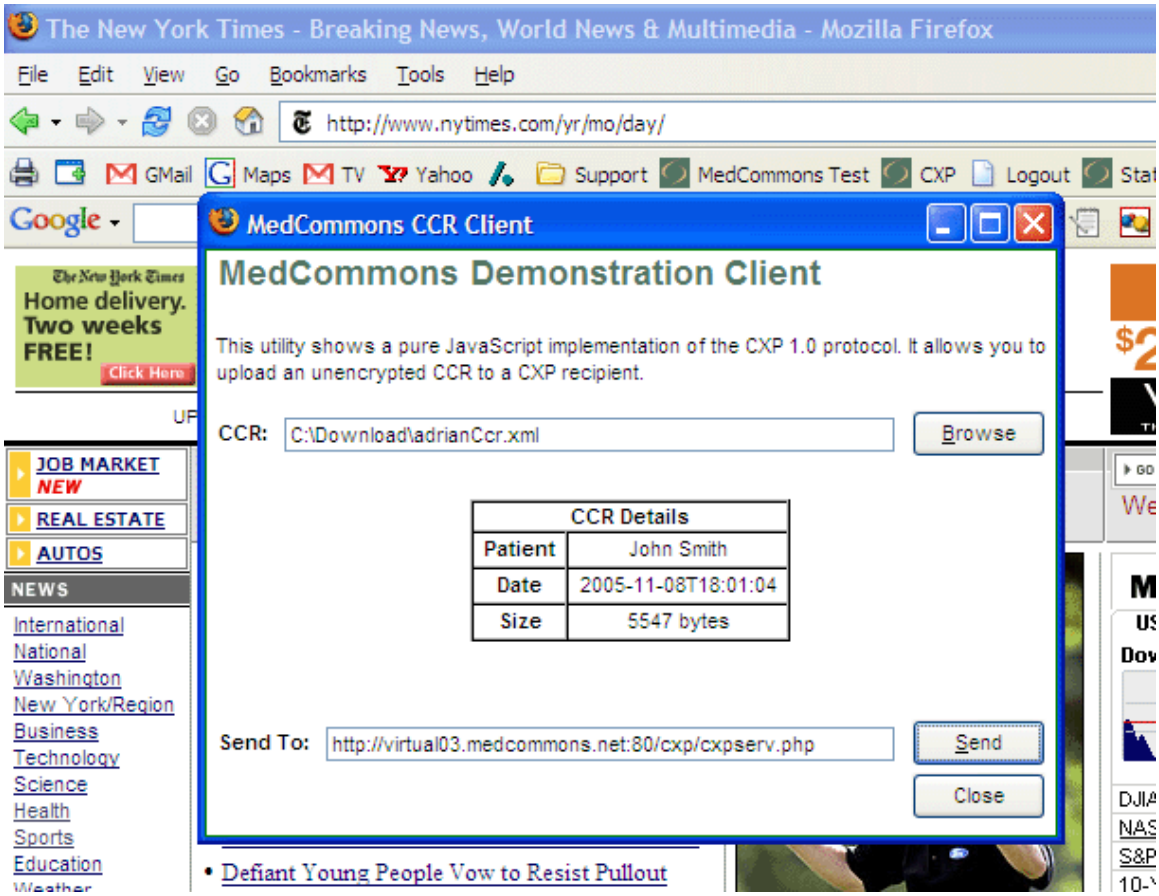
Screens

This section uses screen shots to illustrate one embodiment of the claims:



Screen 1 – Initiate the Transfer from a CCR-aware Application

A user of a standards-based CCR software package can add the capability to send the CCR file to a destination using non-proprietary protocols. In this example, the Send CCR capability has been installed by the user as an extension (plug-in) to their Firefox Web browser. In other examples of the invention, the Send CCR code could have been added directly to another application that is able to create and edit standard CCRs as well.

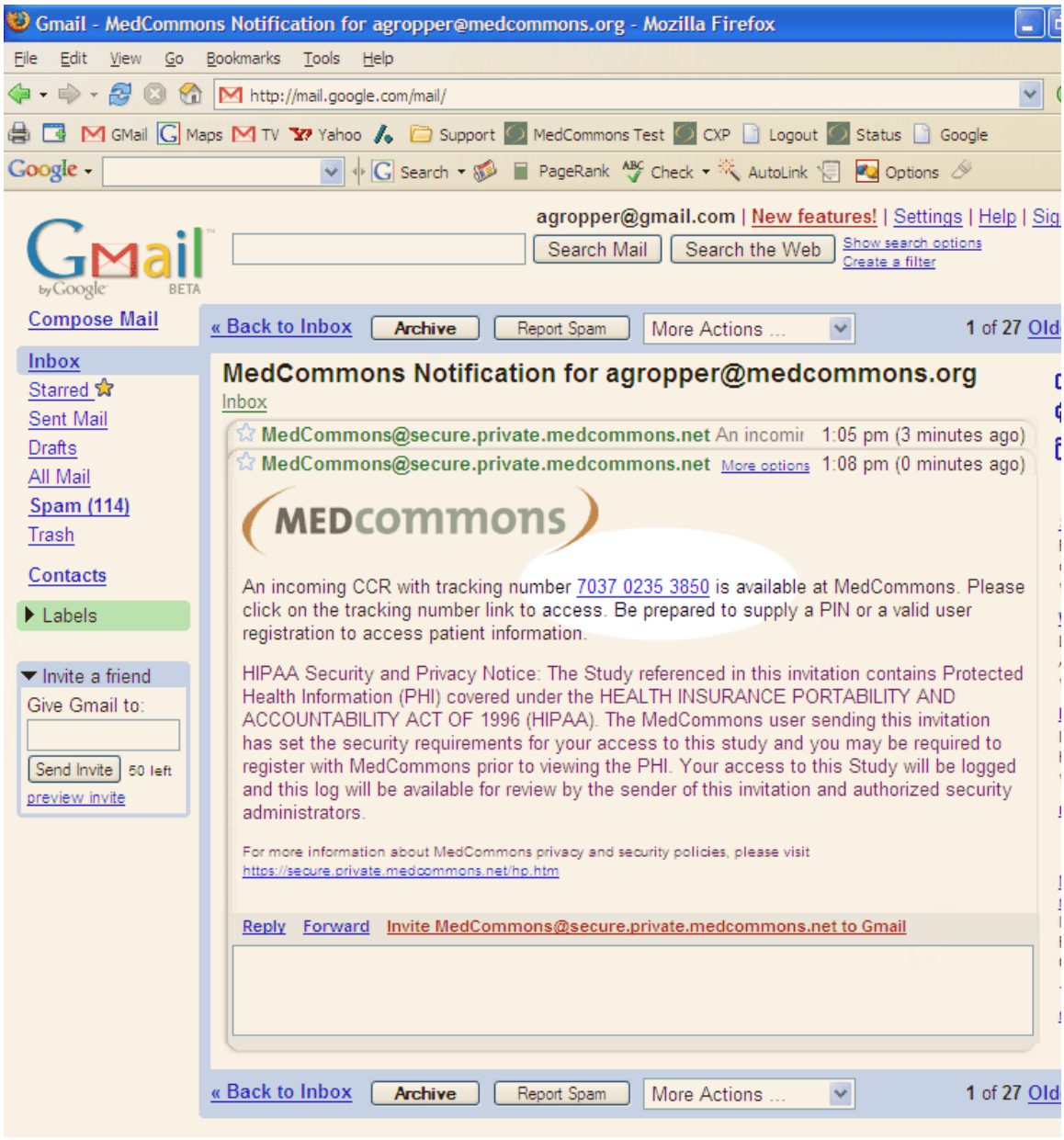


Screen 2 – Browse for the CCR to be Sent and set an intermediary online destination

In other embodiments, this step could be implied by the sending application context and the preset of default online destination such as MedCommons.

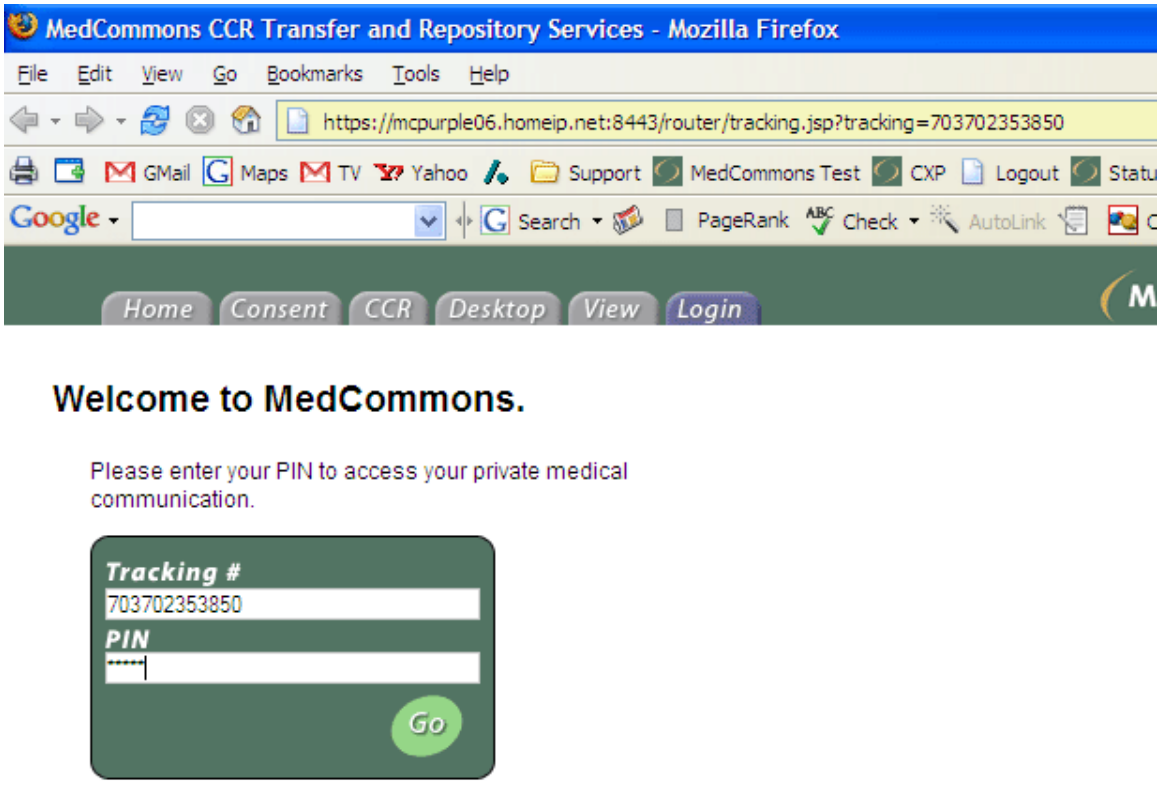
Screen 3 – Note the Transaction ID and Online-Access Authorization Code (PIN)

The combination of Transaction ID and PIN enables an on-line intermediary (including the sending user), if they choose, to access the online copy of the CCR and modify or manipulate the CCR in ways that are not yet supported by the standard. In our example, the user will be going on line to change certain aspects of CCR encryption by manipulating the Privacy Score even though the CCR standard does not yet support the selective encryption feature.



Screen 4 – Optional Notification of a User that the Online CCR is Available

This is an optional feature of the claimed process. The sending user does not need to be notified that a CCR is available online because they saw the Status: TRANSFERDONE (Screen 3). Other intermediaries, most importantly the patient, can benefit from this notification because it gives them an opportunity to divert the CCR for another opinion or to apply a new feature such as selective encryption that is not yet supported by the standard.

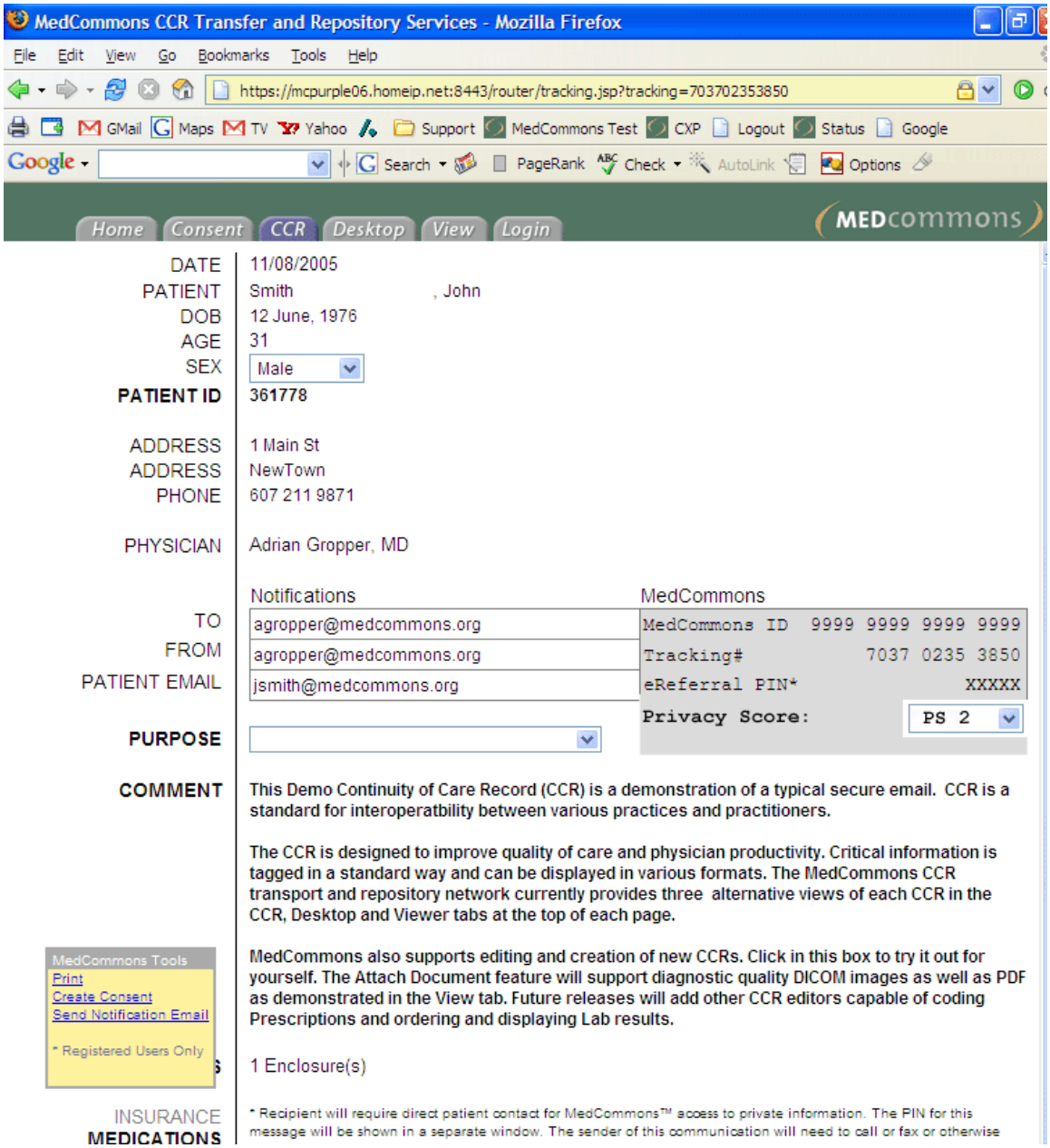


Screen 5 – Authorization Screen

Whether by email invitation or direct access to the MedCommons web site, an intermediary is authorized by the sender when they communicate the PIN from Screen 3 to them. In the simplest case, this is done by telephone and does not involve MedCommons. Other cases include a fax from MedCommons with the tracking number and PIN, a bar code label printed by the Send CCR tool at the time when the CCR is uploaded.

This step is optional in the sense that the CCR may be delivered to the destination automatically and without enhancement or modification.

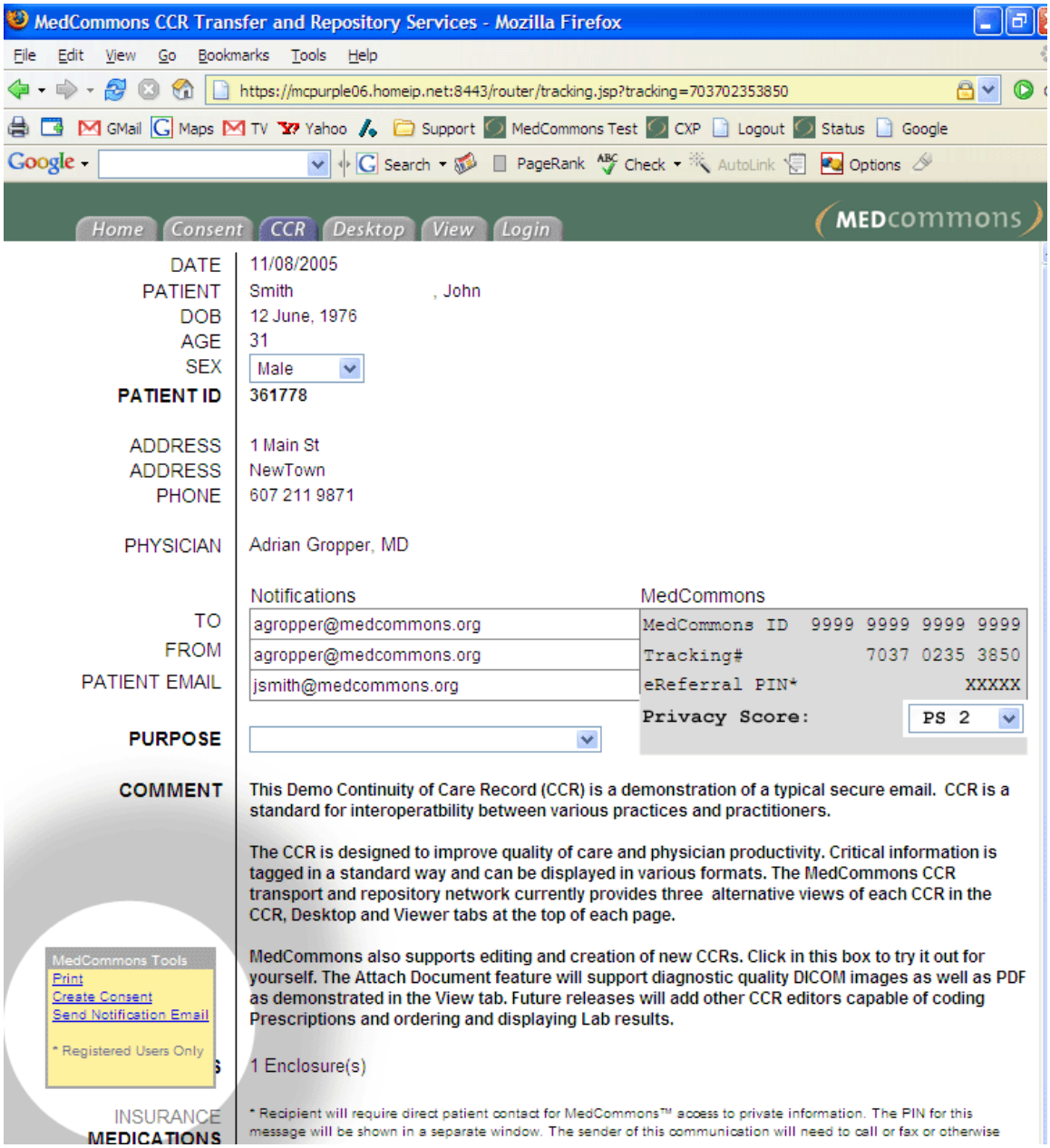
This step is also optional in the sense that some intermediaries that are registered or otherwise authorized by MedCommons could be granted access to selected CCRs without a separate PIN entry step. This would be the case if the sender or patient and the intermediary had an ongoing relationship such as physician-patient. The MedCommons Consent form is a separate enhancement that can be used to establish this kind of implied relationship between the parties.



Screen 6 – CCR Enhancement Example

This gray MedCommons block on this screen shows a Privacy Score selection menu as an example of a non-standard enhancement that can be applied online prior to passing the CCR to its final destination.

For example, a patient might decide that this particular CCR, containing little more than contact, allergies and current medications should be available to all emergency personnel without requiring strong authentication. This choice could be effected by reducing the Privacy Score to PS 2 which would allow MedCommons to transmit the CCR with encryption to another recipient. It is the principal claim of this patent that both the upload of a PIN encrypted CCR to MedCommons and the download of an unencrypted CCR to the emergency physician are standards based whereas the role-based intermediary manipulation may not yet be covered by the CCR standard or may not be supported by the sending system..



Screen 7 – Forwarding of Modified CCR with Notification

This final screen illustrates the final step of the on-line diversion or enhancement process whereby the intermediary sends a standard CCR to the destination by selecting Send Notification Email in the MedCommons Tools.

This marks the end of
METHOD FOR EXTENDING AN INFORMATION STANDARD THROUGH COMPATIBLE ONLINE ACCESS

PDF to CCR Plan

Tuesday, August 02, 2005

1. User sends file to MedCommons via CXP
    1. One way is the CCR Send Tool in FF

2. If the file is a
    1. CCR
        i. it goes into the Unvalidated folder unless it's signed by a key that's covered in a Consent

    2. PDF

        i. it goes to Scansoft OCR and is converted to XML. See ftp://mcpurple05.homeip.net/scrape_in_transit/2005.07.30%2018.03/ for an example of Scansoft output from a sample PDF here: ftp://mcpurple05.homeip.net/Sample_PDF/

        ii. XML is rendered in a temporary window styled to match the PDF as best as possible (possibly using the http://kupu.oscom.org/ technology Simon turned up)
            1. Words found in a MedCommons - wide dictionary (e.g. patient, date ID, number, name) are assumed to be fixed and colored Black.
            2. Unrecognized words (John, 201-555-1212) are assumed to be patient or practice-specific values and are highlighted just like Gmail highlights mis-spellings.

        iii. Continuing the Gmail analogy, as the user mousse over the highlights they can see a list of suggested CCR elements and a choice labeled Ignore.
            1. As the user assigns words to the proper CCR Tag, the highlight changes to **Green** and a sample CCR is populated in the MedCommons CCR or Consent Tab. Mousing over a Green highlight offers displays the formal CCR Tag Name and offers Undo and Ignore as choices.
            2. When the user is done tagging, she is offered to save the template they have created in a special Template Folder on their Desktop along with an image of the PDF to keep everything clear. Templates in this folder can be reopened for editing anytime.

        iv. When a PDF shows up in the Unvalidated folder of the user without a CCR, MedCommons automatically performs the Scansoft conversion to XML as above, does the dictionary scan and, for each Template in the Template Folder,
            1. calculates the RMS distance (the XML has the coordinates of every word clearly pulled out and Robert has already made an XSL that extracts words and their location into a simple table using XQuery) between all words that are present in both the template XML and the new XML.
            2. RMS scores are sorted, and if the least RMD distance is less that a certain threshold, a template match is declared and the user is offered the converted CCR for one-click Validation.

Clinical Data Interoperability for WMC, NYC, HSS and MSKCC

A Proposal for a Continuity of Care Record Transport System

MedCommons Inc.

July 14, 2005

Abstract

Increasing attention is being focused on clinical data interoperability at the community-level (e.g.: Regional Health Information Organizations - RHIO) and beyond toward a National Health Information Infrastructure in support of improved patient-directed care, quality, safety, public health and even national security initiatives. Technical standards are necessary, but it is widely believed that they are not sufficient. A patient-centered approach is also required to provide a new level of trust and customer service and to allow the use of existing HIPAA legal structures that do not support the use of personally identifiable health information for anything beyond direct patient care.

The recently approved Continuity of Care Record (CCR) standard is unique in being driven and controlled by physician practice organizations such as the American Academy of Family Practice, the Massachusetts Medical Society and the American Medical Association and serves the key cross-enterprise interoperability standard role for the current proposal.

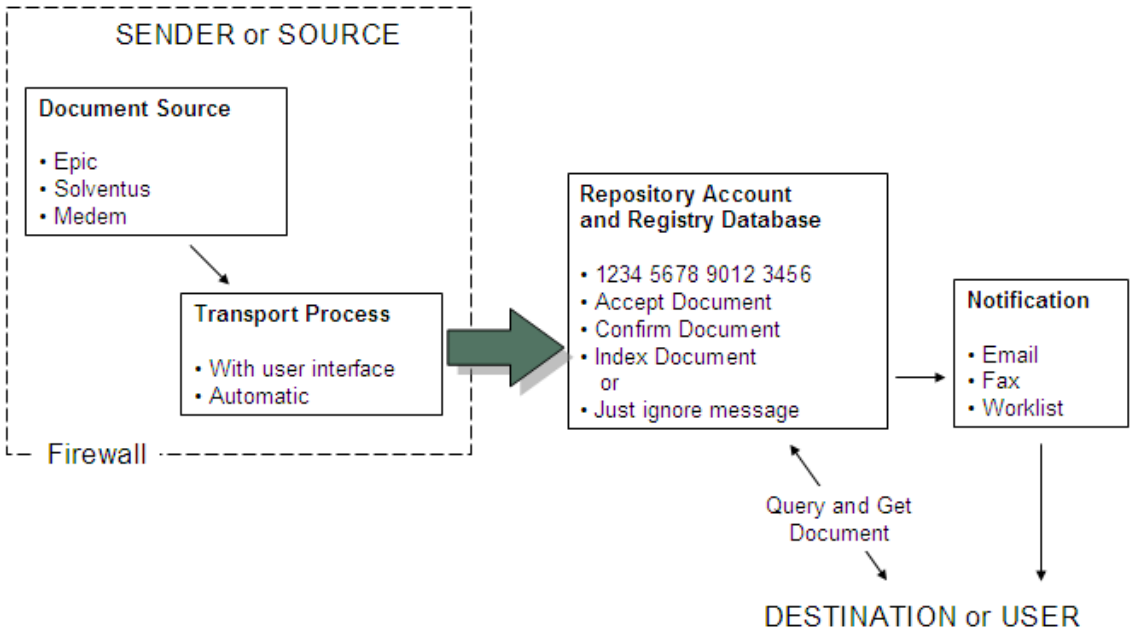


Fig. 1 –Standard CCR Transport Defines the MedCommons Registry / Repository Service

The MedCommons Network adds a patient and physician portal, FDA-cleared diagnostic imaging support, email and fax notification, open source enterprise gateways and HIPAA consent, privacy and security services to create a scalable enterprise and vendor-neutral solution for interoperability across otherwise competitive providers and their competitive information technology vendors.

MedCommons proposes to install and support CCR-based enterprise gateways on the separate networks of WMC, NYP, HSS and MSKCC. Clinicians and administrators at each of these institutions will be able to create CCR-based requests for clinical information from any of the other participants either under the implicit patient consent granted for direct patient care or with explicit consent of the patient for more diverse research, public health and disease management applications.

Unlike earlier attempts at community health information networks, the MedCommons approach is standards-based and accessible to all patients and clinicians in the community. This innovative approach can become the foundation for advanced patient portals and sophisticated disease management services that will extend the reach of clinical research, health promotion and disease management services from these luminary institutions nationwide.

	XDS	**MedCommons**
Open Standards	Yes	Yes
Documents	Unrestricted	**ASTM-CCR**, PDF, DICOM, Others
Notification	Email	Email, Fax
Universal Transport	No	Yes
Patient Accessible	No	Yes
User Portal	No	Yes
XDS Interoperable	Policy Dependent	Policy Dependent

Fig 2 –IHE-XDS and MedCommons are Interoperable Registry / Repository Architectures Designed for Community-wide Medical Communications.

Technical Approach

Interoperability across institutional boundaries serviced by disparate information technology vendors requires simple yet effective standards that address real-world privacy and systems integration practices. The RHIO concept of a community-managed registry pointing to associated private document repositories is currently at the fore of interoperability discussions. IHE-based Cross Enterprise Data Sharing (XDS) is being put forward as one candidate for the family of standards around which a vendor-neutral RHIO could be built. However, XDS is based on complicated and still evolving Web Service standards and leaves unresolved HIPAA privacy issues that have made cross-institutional registries economically unsustainable because there's no clear way for insurers or vendors to mine the data.

MedCommons proposes a functionally compatible alternative to XDS based on the ASTM-CCR standard as a solution to the interoperability problem. MedCommons and other competitive CCR transport service providers will act as a - FedEx-like - as a common carrier between enterprise information systems. This CCR-centric approach is much simpler than XDS and does not raise the privacy issues that XDS has yet to address because it is patient-centric and fully consistent with HIPAA as it stands today. Nonetheless, the MedCommons-proposed architecture is fully IHE based inside an enterprise and will interoperate with standards-based community repositories including those based on IHE-XDS.

MedCommons provides interoperability services to enterprises, systems integrators and healthcare IT vendors via standards based interfaces:

- A simple , scalable and secure document transport interface based on the established and widely deployed WebDAV protocol,
- A cost-effective temporary repository for documents in transit between institutions backed by HIPAA compliant privacy, tracking and customer support systems,
- A universal email and/or fax-based notification service that can be used to address consent and privacy issues with patients and to alert practitioners of new documents,
- A commitment to open standards backed by our policy of open-source software for IHE-based enterprise integration gateways.

Adding patient-centric interoperability to your enterprise involves a number of steps that can be deployed as standard interface by your technology vendor or across IHE interfaces to an open source MedCommons gateway:

- Identify patients as you normally do within the sending institution (no additional cost),
- Export ASTM-CCR to a secure WebDAV folder managed by MedCommons,
- Process and save the MedCommons patient and tracking identifiers to check for errors
- Register with or poll MedCommons for status changes on the transfer (optional),
- Validate and import incoming CCRs delivered by MedCommons (optional).

- **CCR** An XML document conforming to the CCR standard Schema and labeled with the CCR-standard document ID (can be signed and/or encrypted per the CCR standard). There are up to three parties to the CCR, the sender, the recipient, and the Patient.
- **Consent** A document that establishes a relationship between a CCR sender and a Patient under HIPAA. The CCR destination may also be a party to the Consent and thereby allowed automatic delivery by MedCommons. At least one party to the Consent (sender, patient, destination) must have a paid MedCommons Account ID. Consents are stored and indexed by MedCommons and may be associated with X-509 Certificates for enterprises and individual. Uses the patient information required in a CCR header along with source information (if any) to create a new 16-digit MedCommons ID for a patient and a subdirectory with that ID the WebDAV Dropbox.
- **Dropbox** A secure MedCommons managed WebDAV folder, shared between a remote user or computer and MedCommons. The WebDAV folder contains a subfolder named with the MedCommons Account ID. MedCommons provides errors and warnings including:
  - Account Directory Created by sender using WebDAV –the sending system already had stored a MedCommons Account ID for this patient or destination based on a previous Consent.
  - Account Directory Missing – please create an account by supplying a Consent
  - File Corrupted – please retransmit
  - File Accepted – Use Account ID and CCR ID to track status.
- **Status Service -** A MedCommons Service that accepts Account ID and CCR ID and returns the Tracking Number and MedCommons Status. No PHI other than the Account ID is transferred. The requesting party needs to be a party to the Consent. This is an automated alternative to the Tracking Number box on the MedCommons Portal where a PIN or Account ID (as defined by Consent) will be required along with a Tracking Number.
- **Notification Service -** A MedCommons Service that sends email or faxes to the parties listed in a Consent:
  - Emails contain no PHI whatsoever, just a MedCommons Tracking Number link.
  - Faxes reproduce elements of the Consent as a cover sheet and may include some or all of the CCR content as allowed by the Consent. The PIN is also shown on the Fax cover sheet. Faxes are full of PHI and must be secured just like any other medical fax.
- **Portal** MedCommons provides an online portal where users with paid Accounts or a Tracking Number and PIN can check Status, View, edit and forward the CCR along with its PDF and DICOM attachments; and create new consents.
- **Gateway** A MedCommons-supported collection of open source software components that:
  - Install on a MedCommons CCR user's LAN as an appliance or a Windows XP service
  - Uses a valid X-509 Certificate to identify itself to MedCommons as party to a Consent that authorizes automatic push delivery. A certificate may be generated by MedCommons, Verisign, or another approved CA.
  - Automatically pre-fetches CCRs and attachments to a local file system and, optionally, performs required IHE Transactions with on-site systems.

Integration

1 – Gateways

Each institution will install a MedCommons Gateway server as a demarcation point between the LAN and the MedCommons network. This box will use IHE (Integrating the Health Care Enterprise) standards and profiles to communicate with the interface engine and secure personnel directories of each institution. If required, the MedCommons Gateway administrators become the default information support agents for automatically processed CCRs to supplement the specific CCR transfer requests attributable to specific individual clinicians.

Other functions of the MedCommons Gateway include support for document and image pre-fetch to avoid network delays, local caches of Master Patient Index (MPI), patient consent registry and security audit logs.

All transfers in or out of an enterprise gateway are encrypted and mediated by a secure MedCommons server and are backed by Verisign-registered X-509 standard certificates at both ends (TLS). For additional security, MedCommons stores all protected health information on redundant encrypted servers using different keys for each patient and keeps these keys on separate servers at separate locations. This means that no single-point compromise of security will yield information on more than a handful of patients.

2 – Patient Identifiers

For lowest cost and maximum ease of use, MedCommons adopts the CCR practice for patient identifiers and allows each institution to identify patients per legacy practice. Behind the scenes, MedCommons provides the Consent document as a patient-centric way to clearly and voluntarily associate the patient's identifiers across institutions that are party to the Consent.

The Consent also provides patients the option to specify a separate MedCommons Account ID that they can control for use as the basis of their Personal Health Record (PHR) for emergency access world-wide, second opinions and long-term archiving of sensitive diagnostic, family and genetic history.

The involvement of the patient in the Consent process via MedCommons supplied interfaces, secure Web portal, email and fax notification services provides the institutions with a high level of protection under HIPAA and allows the patient an entry point into paperless referrals and patient-directed care.

In addition to the Consent, MedCommons will provide MPI integration services to each institution as an extra-cost option.

The Consent mechanism is recommended but not required. Each institution can choose to allow CCR-based transfer of patient information under the blanket HIPAA agreement that patients typically sign for clinical care. This feature may require access to institutional user directories and strict monitoring of security logs by the institution.

3 – External Parties

Beyond the four principal institutions and their patients, MedCommons provides a standards-based and vendor-neutral interface to reference labs and diagnostic imaging services. Some insurance plans, decision support and disease management services are also expected to develop CCR-oriented interfaces that are integrated with the MedCommons transport and HIPAA security network services.

Interfaces to value added networks such as Quest or RxHub will benefit from advanced interface tools such as TruData and will be priced separately as desired.

4 –Secure Email Functionality

MedCommons includes a CCR-standard based secure email capability for patient-provider communications. In many cases this capability will be preferred over proprietary secure email approaches because of lower cost and better integration with other information systems.

5 – CCR Creation and Interfaces

MedCommons will support all CCRs generated by any on-site systems and will offer user-interfaces to create CCRs as required.

In addition and at extra cost, MedCommons will create specific HL7 interfaces for conversion of Computerized Patient Order Entry (CPOE) and other patient data feeds in order to reduce data entry and improve productivity and patient safety.

On the CCR import side, MedCommons will support IHE-based profiles for automated processing of cross-enterprise data as these are developed and approved.

6 – Automated Consent Creation

MedCommons will automatically derive a Consent form – ready for patient signature – based on CCR header information and will assist in the creation of new CCRs on the basis of previous CCRs or existing Consent documents.

MedCommons Consent documents will clearly identify the patient including historical maiden names and previous addresses..

The Consent also identifies the clinical participants to the interoperability transaction and will allow access and review of security certificates while providing a clear and convenient statement of enterprise policy and terms of-use. Provision will be made for inclusion of license, UPIN and DEA identifiers along with their corresponding expiration dates.

Enterprise-specific branding with logos and provider's business cards will be supported.

The Consent mechanism is inherently bi-directional and a single Consent can serve for ordering information from an institution as well as the response that provides that information.

7 – Notification

Based on parameters in the Consent and each CCR transaction, MedCommons will notify each participant, including the patient, via email or fax.

For low cost and universal reach, emails are standards-based and reveal no PHI whatsoever.

For maximum interoperability as allowed by HIPAA and workflow convenience for participants without electronic health records, faxes can include PHI and can reference the digital versions of the CCR and attachments available on the MedCommons portal.

Optional at additional cost, MedCommons Gateways can be configured to integrate Notifications of CCR-based activity with IHE standard workflow profiles.

8 – Personal Health Records

MedCommons will offer to patients management and archival storage of their personal health records based on the CCR standard. Patients will not be required to participate and can always access their CCRs and attachments cost free for one month. MedCommons is a patient centric service and will make every effort to develop sponsors to support those patients that cannot afford the $50 per year that a typical PHR is expected to cost.

Patients will be able to use their PHR accounts to make CD and USB Flash Memory Token copies of selected CCRs and attachments as well as manage a subset of their PHR information with key emergency information such as allergies, family and clinical supports.

Application and Policy Profiles

MedCommons is an independent, multipurpose network for private patient data that includes both portal and archival storage services for patients and other account holders. MedCommons technology and policies attempt to be flexible and neutral to accommodate the widest possible range of users and to provide the benefits of broad interoperability "network effect" to users.

Privacy and interoperability are not natural allies. MedCommons promotes interoperability by providing a range of clear and effective opt-in options for our users, including direct patient notification and using the patient as an intermediary to a referral.

The sections that follow present some of the profile options that users of the MedCommons network will need to make as they connect to the network.

Document File Types

MedCommons portal, user interface and broad interoperability features are designed around ASTM-CCR, PDF and DICOM file types. Other types, such as HTML or Microsoft Word can be accommodated but introduce security and privacy risks and can increase support costs when appropriate viewers malfunction. In addition, multiple document formats increase the cost of archival storage as digital formats evolve rapidly over time. MedCommons recommends converting structured patient data to ASTM CCR (XML) and narrative documents to PDF. DICOM is the uncontested medical image standard.

1 ☐ List document types other than CCR, PDF and DICOM you will transfer: _____

2 ☐ Will MedCommons portal and archive users be able to view and sign the additional document types? _____

Confirmation Code

MedCommons acknowledges responsibility for a document by issuing a Tracking Number. This Tracking Number is key to our ability to provide status updates and technical support. How will the sender receive the Tracking Number?

3 ☐ Email or Fax Number address supplied in the CCR

4 ☐ Secure HTTP Connection to MedCommons accepts the Tracking Number for storage in sender's information system.

5 ☐ Other. Please Specify: _____

6 ☐ None. Tracking of transfers will be the patient's or the destination's responsibility.

Encryption, Status Queries and Retrieval Criteria

MedCommons acts a registrar for the documents it transfers. This allows us to connect users without formal business agreements while fulfilling HIPAA and other legal requirements. As a transport agent, MedCommons wants to protect the privacy and confidentiality of its users. Therefore, our services are available to users who encrypt their documents with keys that we do

not control and to anonymous users. Encryption and anonymity raise costs and may lead to patient safety issues so they are not recommended as a default policy.

7 ☐ MedCommons will store a copy of the encryption key by default. (Recommended)

Even for encrypted documents, a registry indexes information about a document and its customers to enable status queries and document retrieval. MedCommons default document identifiers are 160 bit pseudorandom numbers (GUID) that reveal no information about content, source, destination or patient. In addition to the GUID, MedCommons will index and respond to queries based on:

8 ☐ 16 digit MedCommons Account ID - a voluntary identifier for physicians or patients who have paid MedCommons accounts. A bank account number is a common example of a voluntary ID.

9 ☐ CCR Standard Identifiers including CCR_Document_ID, and CCR_DateTime.

10 ☐ Additional identifiers such as practice-specific patient identifiers. Specify source.

11a ☐ CCR Element Tags: _____

11b… add sheets as needed.

12a ☐ Others: Tag Description _____ and Source _____

12b… add sheets as needed.

Authentication and Authorization of Users

13 ☐ Site will provide user directory for MedCommons use. Specify _____

14 ☐ Site provides identity server with SSL certificate. Specify _____

15 ☐ Users will have paid MedCommons accounts

16 ☐ Users will have temporary (free) MedCommons accounts

17 ☐ A third-party identity provider will be used. Specify: _____

Notification of Users

MedCommons notifies users and patients as needed for both workflow and security purposes. Primary notification is via email or fax. Additional notification methods are available at extra cost.

18 ☐ Telephone notification option. Number in CCR Element _____ or Specify _____

19 ☐ Other notification. Specify: _____

Additional Privacy Requirements

MedCommons will try to accommodate your additional privacy and security requirement. Please specify any additional requirements for document and registry information expiration, document deletion, administrative override and administrative access to security logs. Also specify MedCommons audit requirements.

MedCommons Use Case – Inbound Content Handling

This document is a summary of a conversation between Adrian and Simon to describe changes that will be made to the MedCommons Gateway platform to add features and functionality supporting handling of inbound content to a user's desktop.

The document is presented as a walkthrough of two use cases with specific notable changes to the current system highlighted in various places along with technical notes inserted as italics.

Use Case 1: Sends CCR via MedCommons ID

The ability to send a CCR to another (or the same) person's MedCommon's account will be added.

Context

The starting point for this use case is that a user (we will refer to them as a patient, but there is nothing specific to patients here, it just matches the scenario better) receives email with tracking number link. They also receive a PIN for accessing the corresponding CCR.

Flow

1. Patient clicks link in email
    a. System displays screen showing tracking number field (filled) and PIN field, View button
2. Patient fills PIN, clicks View button
    a. System displays desktop showing the single CCR corresponding to the tracking number.
    b. The tool palette has a "New Transmission" option
3. Patient clicks "New Transmission"
    a. System displays CCR tab showing CCR details including "To", "From", and "Patient" fields. The "To" field is blank at this point.
4. Patient edits any details as desired on page and fills a MedCommons Id in to To field.
    a. Upon tabbing off the field, gateway displays message "Warning: sending a CCR by MedCommons ID may compromise your information if you enter the wrong ID. Please re-enter the desired MedCommons ID to confirm:". A field is displayed for the user to enter the MedCommons Id
        1. *Note: the patient could have put an email address in the same field, or a fax number. For these other options the warning message is not displayed. However other than user interface effects, the gateway does not behave visibly differently for these different options, it simply passes the field to central as free text. Central is responsible to recognise and appropriately handle the notification based on the type of To field*
            a) *Note on the Note: I am not sure this statement maps to the fields in the CCR. While the same field may be passed to Central notification service regardless of what is filled in To, there are explicit fields in the CCR for email, fax, and MedCommons Id and presumably these should be filled appropriately depending on what the user enters. In this case the gateway would be performing this function. In both cases some intelligent parsing is going to be required to interpret this field.*
        2. *Note: the MedCommons Id should accept flexible format for the id – eg. The ID could be prefixed by "#", "Id", "MedCommons Id" etc. However the ID should contain 16 digits to be recognised.*
5. Patient re-enters MedCommons ID matching the original in the provided field.
    a. System accepts MedCommons ID into To field

6. Patient click's "Send Notification"
    a. System displays confirmation that notification has been sent including Tracking number and PIN. (*This is nearly the same as operation is now, except probably there should be no option to send email since no email was provided)*

Use Case 2: User Recieves CCR Sent by MedCommons ID

Context

The context for this use case is that a user (this could be any kind of user, physician, patient etc.) logs in to see their desktop. A CCR has been sent to them as per Use Case 1. The user's desktop prior to Use Case 1 was empty.

Flow

1. User navigates to secure.medcommons.net, clicks "logon" tab, enters their user name and password and clicks "Log on"
    a. System displays user's desktop. The desktop contains a single folder with large stripes on it. The folder is labelled "Unvalidated". It does not have a date on it.
        i. *If there were other folders on the desktop representing existing CCR's belonging to the user then the abovementioned folder would be on top of the other folders*
    b. An open folder is displayed representing the Unvalidated folder. The open folder does not have any of the normal CCR information seen for other desktop folders, rather it has only thumbnails.
        i. The thumbnails are grouped in some way. Maybe rectangular border, or background shading or some other method. In this way content composed of multiple thumbnails that is received by the gateway as a unit is displayed visually to the user in the same group unit as it was received. In this example use case there is only 1 group because the user's Unvalidated folder was empty prior to receiving the CCR from Use Case 1.
    c. Desktop contains tools palette with "Create CCR" option
2. User clicks one of the icons for the content in the open folder on the desktop
    a. The group for the icon highlights
        i. *Note: by implication, this will mean that the viewer is not going to open on the first click on an icon as it does for other folders on the desktop*
3. User clicks "Create CCR" option in Tool Palette
    a. System generates a CCR based on the content of the group that was highlighted by the user.
        i. *The heuristic used to compose a CCR might work as follows:*
            1. *if the user already has CCR's on their desktop then use the most recent CCR as a base. If there is a CCR in the group, compare the patient name, age and sex on the CCR with those specified in the current CCR. If the information conflicts show a warning to the user, and accept the old information. NOTE: the new information from an inbound CCR is NOT incorporated into the new CCR in this case. It only generates a read-only warning to alert the user.*
            2. *If there is no existing CCR on the user's desktop, generate a new CCR based on a) any CCR contained in the highlighted group and/or b) any information that can be harvested from any DICOM content in the highlighted group*
    b. System switches to Viewer tab and shows the group that was highlighted by the user in the Viewer. The CCR generated in part a. above is shown as thumbnail 0 at the top of the thumbnails.

c. The Tools Palette has options “Edit CCR”, “Create CCR”, “Discard CCR”, “Cancel”

4. User clicks “Create CCR”
    a. System creates and saves the CCR generated in 3.a to the user’s desktop. All references are saved as part of the CCR
    b. System switches back to Desktop tab. The new saved CCR is displayed as a folder and the original group of icons highlighted by the user in 2. are visible as thumbnails. The CCR is open on the desktop. *Note the CCR is open because it is the only CCR. If there were pre-existing CCR’s it would still be open because it would be the most recent.*
        i. *Note: since this was the only unvalidated CCR, the Unvalidated folder is now not present on the desktop, because it would be empty. However if there were other unvalidated content the Unvalidated folder would still be present, but would no longer contain the group just validated by the user. The Unvalidated folder would be the top folder in the stack and would be open in this case.*
5. [**alternative path to 4]** User clicks “Cancel”
    a. System displays desktop. Desktop appears as it did when they first logged in Step 1.
6. [**alternative path to 4,5]** User clicks “Discard CCR”
    a. Warning is displayed indicating CCR will be deleted.
    b. System returns to Desktop. The desktop is blank.
        i. *Note: the desktop is blank because there was no other content and the user has discarded all the content in the Unvalidated folder. The Unvalidated folder does not display when it is empty.*

DICOM Capture UI Proposal
V0.1 - June 23, 2005

1. DICOM Capture requires Win XP
2. Sender uses IE or FF to open an account. Gives Credit Card info.
    a. Pays $50 to cover Registration for FDA reasons and 3 uploads.
    b. After that, it's $30 / three uploads.
    c. Tech support is $50 / incident unless it's our bug.
3. Registered Sender downloads installer.exe
    a. Runs installer
    b. Agrees to Terms of Use. DICOM Uploader is Open Source Software. Source is at www.medcommons.net/sources
    c. MedCommons DICOM Uploader Installs and runs automatically and at startup
4. DICOM Uploader appears as a System Tray App
    a. The Sender's MedCommons ID is automatically derived from the installed certificate or some other automatic way.
    b. The IP address is retrieved from Windows
    c. An AEtitle is autogenerated based on the initial characters user's last name and the last two digits of their MedCommonsID
    d. The DICOM port is preset to 104
    e. The IP / AETITLE and Port are displayed when the sender rolls over the system tray icon.
5. The sender calls the Modality Tech and reads off the IP / AETITLE / PORT (often, the Tech will be the Sender)
6. Modality Tech sends a study via DICOM.
    a. Study is placed in the Sender's Inbox Folder on the Sender's Desktop
7. Sender may or may not waits for the DICOM transfer is complete
8. Sender Logs In
    a. Clicks Desktop Tab
    b. If no more DICOM appears for 1 minute, a series is closed and an icon appears on the side of the Inbox Folder. It's up to the sender to wait long enough for all of the series to upload.
    c. MedCommons groups all of the Series that belong to a single Study together.
    d. Clicking on any Icon in a Study loads all Series for that Study in the Viewer and launches the Viewer with DICOM overlay On by default.
    e. An alert dialog box appears on the left side of the Viewer. It lists all of the patient demographics from the DICOM header and offers three choices:
        i. Create CCR for this Patient / Study
        ii. Delete this Study from Inbox
        iii. Cancel – leaves Study in Inbox
9. Sender chooses Create CCR
    a. Enters or Changes Patient Demographics including Name, DOB, Sex, MRN, MedCommons Patient ID as available –
        i. Save is automatic and a new CCR with the Study appears on their Desktop.
        ii. An alert is generated if MedCommons automatically generates a provisional MedCommons ID for the Patient.
        iii. A Tracking Number is assigned
    b. Enters notification emails or fax numbers – Save is automatic – The Tracking Number doesn't change
    c. Optionally – clicks on and prints Consent for the patient to sign.
    d. Clicks Sign CCR and Fax or Sign CCR and Send Email
        i. HIPAA Log for the Tracking Number changes Status to reflect the conversion to fixed content. No further changes are allowed.
10. Recipient uses PIN to view the CCR and attached DICOM
    a. DICOM Download to a workstation or PACS comes in a future release.

Order CCR – Response CCR
August 13, 2005

1. Patient Demographics on Screen in some App.
    a. In MedCommons, user may have entered info into CCR tab
    b. In MedCommons, user may be looking at an old CCR in CCR tab
    c. In other app, user may have never touched MedCommons
2. User clicks Create CCR
    a. On MedCommons Tools floater
    b. On CCR – compatible other App.
    c. Implicitly by Print to MedCommons CCR Creation Folder (stores as PDF)
    d. Implicitly by Faxing a form to the MedCommons drop box
    e. Implicitly by copy and paste into CCR Tab
3. A CCR Appears in MedCommons or another CCR Editor App.
4. User launches proprietary Order editor supplied by VAN Vendor.
    a. Using live hierarchical menu in MedCommons
    b. CCR sections are inserted and validated as VAN Order presets.
    c. User checks and edits notification options.
    d. User accepts CCR Purpose: Order
    e. User enters CCR Comment narrative if any
    f. User checks off sections of previous CCR to be included (e.g.: Insurance). This might require opening previous CCRs - in MedCommons this is done using live hierarchical menu mega gesture.
    g. User accepts Terms of Use by checking box.
    h. User Signs CCR.
5. A Credit card processing option may fit here
    a. Physician reimbursement for consultation
    b. Lab fee payment
    c. Co-payments
    d. Deduction from HSA
    e. Pre Certification by Payer / Insurer
    f. MedCommons gets a cut
6. User Clicks Consent tab
    a. Missing MedCommons patient ID triggers warning.
    b. User enters or accepts provisional patient ID
    c. User prints consent for Patient signature and files a copy.
7. User clicks Export CCR (to MedCommons)
    a. In MedCommons this is on the Tools floater.
    b. A confirmation is returned
    c. HIPAA Logs are updated with new status: Sent
8. MedCommons Notifies all parties
    a. Email or Fax
    b. CCR gateway dropbox to a trusted system on LAN or VPN
    c. CCR dropbox on WAN via https WebDAV
9. CCR To Recipient opens Order CCR
    a. Processes Order as above
    b. Patient identifier mapping into local system is the recipient's problem.
    c. Other CCR Edits and presets manipulated manually or automatically is above.
    d. Creates Response CCR that references Order CCR (in a standard way).
    e. Exports Response CCR using MedCommons or equivalent
    f. Attaches DICOM or PDF documents using MedCommons
    g. Clicks Export CCR
10. Med Commons Notifies parties to CCR and Consent
11. Order creator and Patient both get a copy of Response CCR.
12. Note: Response CCR integrates the results based on the intent of the ordering physician thereby making the CCR more valuable and much less complex than typical EMRs.

MedCommons Business Summary
August 10, 2005

What

MedCommons is a branded, standards-based value added network for transfer, archiving and indexing of medical documents including orders, images, reports and records. MedCommons introduces new technology that, for the first time, enables patients, physicians and enterprises to share the same service technology regardless of the specific policy choices of each client. The policy-neutral design of MedCommons enables, in turn, the creation of Affinity-Driven Health Networks alongside and interoperable with more traditional Regional or Community Health Information Networks. Inherently national in scope, Affinity-Driven Health Networks are not subject to being overwhelmed by local political or managed care interests and can provide a distribution channel for national-scale diagnostic, decision support and disease management services. A white paper, in progress, is attached as Appendix A.

MedCommons services compete in the personal health record, provider and service organization portal and interoperability network services markets.

Additional information and a product demonstration are available at http://www.medcommons.net

I think it was a Slashdot pundit who offered: "XML is like violence, if it's not working for you, you're probably not using enough of it." The same might be said of managed health care as regional cartels design to do more to control the behavior of physicians and patients even as it's become clear that such management can no longer contain healthcare costs.

MedCommons is not just another health IT vendor pandering to managed care:

- Patient Privacy (Independent and un-conflicted, like a bank)
- Open Standards Throughout with Open Source Enterprise Components
- Corporate Employers and Professional Organizations as Customers and Sponsors
- Universal Access Principle (Free, Individual and Enterprise Users are all supported)
- Designed to become the de-facto standard for transport and privacy interfaces, not a practice management system
- Simple CCR standard plus bland, open XML control structures encourage reuse and innovation
- A wide range of clear and interoperable policies are set independently by MedCommons clients:

  Typical Policy Categories and Choices
  - Clone existing affinity group policy or to create a new one
  - Opt-in mechanism available to patients
  - Notification of patient when implied consent is used instead of opt-in.
  - Type of Global Identifier: National, Biometric, Probabilistic (MPI) , Voluntary
  - Constrained Document Set
  - Constrained Vocabulary
  - Patient allowed independent access and copy
  - Direct or sponsored payment vs. institutional bundling
  - Point-to-point option without any archival side effect
  - Paper and fax allowed
  - Document retention and deletion
  - SAML interface to enterprise directories for automated registration of enterprise users, roles and delegation
  - Automatic import validation criteria

When

MedCommons has been in development for some two years and is now entering clinical use. Our roadmap began with FDA clearance for our diagnostic imaging component in July 2004[1]; followed by participation in the HIMSS Cross-Enterprise Interoperability Showcase in February 2005[2]; and a featured presentation at the inaugural CCR Developer and User Conference in June 2005[3].

The first nationally accessible clinical MedCommons system, the POPS project, will be introduced to individual primary care practitioners in September 2005. Our first enterprise-system for nationwide medical image transport to a processing laboratory will be introduced in October 2005. The American Academy of Family Physicians will introduce the first Affinity-Driven Health Network in November 2005 and is expected to include the first direct interfaces between commercially available electronic health record systems and MedCommons.

How Much

The market for networking of health record systems in the US is $156 Billion over 5 years[4]. The functionalities section of this paper is reproduced verbatim in the text box and shows the range of domains that account for the overall figure. The paper also estimates that two-thirds of the cost will be for additional functionality and one third for interoperability.

MedCommons will play a role in most of the key domains and in both additional functionality (archiving, display) and interoperability (transport, indexing, and privacy).

Functionalities

The panel also identified a set of critical functional domains for a model NHIN: inpatient and ambulatory result viewing, inpatient and ambulatory electronic health record (EHR), inpatient and ambulatory CPOE, electronic claims submission, electronic eligibility verification, secure electronic patient communication, and electronic prescription acceptance by pharmacies. In general, each of these functional domains was relevant for only a subset of the key providers.

We describe these functional domains in more detail in another paper (16). Briefly, results viewing allows electronic viewing of test results, such as laboratory tests or radiologic examinations. Electronic health records are computerized systems that maintain relevant health information, including electronic charting. Computerized provider order entry refers to an application that allows all medical orders to be entered electronically. Electronic claims submission and eligibility verification are methods of computerizing communications with third-party payers. Secure electronic patient communication refers to computerized e-mail or messaging systems that allow private communication between patients and their health care providers. Finally, pharmacy electronic prescribing refers to the ability of a pharmacy to accept electronic prescriptions. The expert panelists achieved very good consensus during the development of a model NHIN.

[1] http://www.**fda**.gov/cdrh/pdf4/k041326.pdf

[2] http://www.interoperabilityshowcase.com/2005/

[3] http://www.centerforhit.org/x1311.xml

[4] **Kaushal R**, **Blumenthal D**, **Poon EG**, **Jha AK**, **Franz C**, **Middleton B**, **et al.** The costs of a national health information network. Ann Intern Med. 2005;143:165-73 – Appendix B

What is a MedCommons Account?

MedCommons principal revenue source is the sale of accounts. Each account is represented by a 16-digit MedCommons ID and belongs to a single individual. Individuals can have as many accounts as they feel that they need but MedCommons design aims to keep this number to a minimum by reassuring the individual that their MedCommons Desktop (which represents an account) is visible to them, and them alone. Future upgrades to MedCommons will facilitate custodial control of accounts by parents, children and legal guardians.

Each MedCommons account is associated with some amount of private and secure on-line storage managed by MedCommons on the individual's behalf. – like a safe deposit box. To further enhance trust, on-line accounts can be mirrored to a physical storage appliance such as a USB memory stick that is physically in the account holder's possession. MedCommons will resell such storage appliances for both patients and physician practices, and the software in them will be open source.

The individual that controls each MedCommons account (be it paid for directly or sponsored by their employer) can configure a broad range of policies and choices that are applied by MedCommons as custodian for that account. Many of these are described in the first text box and others will be added based on market demand. The primary purpose of these customizations is to control how MedCommons responds to queries about an account and whether information can flow automatically in or out of an account. Future releases will enable increasingly sophisticated linkage of policies across accounts to enable shared worklists and backup users to take call for a vacationing physician, etc…

MedCommons will derive revenue from both individual and enterprise accounts. Individual accounts will compete in the emerging market for Personal Health Records (PHR)[5] while enterprise accounts will focus on networked suppliers of diagnostic and management services to the health care industry. In contrast to Electronic Health Record (EHR) vendors, MedCommons will avoid charging individual physicians or small group practices and will seek sponsorship of individual patient and physician accounts from employers and professional organizations respectively.

To date, MedCommons has been funded with an investment of $ 1 million by its founders directed primarily at software development and standards participation. Our cash burn rate averages $35,000 / month. We now seek an additional $XX million to fund call-center support of revenue-generating operations, complete our management team and to fund marketing and public relations efforts.

Where

MedCommons is a distributed, Internet-based operation with key offices in New York and Massachusetts. Developers and support personnel work from home offices. The majority of our servers are rented as dedicated "root" servers from commodity Internet hosting providers and managed by MedCommons systems administrators. Location redundancy is inherent in our design. Security is provided by encryption in transit and on disk with encryption keys stored separately from encrypted data.

Some of the additional funds will be used to lease secure hosting for the company's most security and mission-critical systems. Encrypted medical document storage will continue to be distributed among Internet-hosted commodity servers with support for storage appliances on the customer's site as an added-cost option.

[5] **The Role of the Personal Health Record in the EHR**
http://library.ahima.org/xpedio/groups/public/documents/ahima/pub_bok1_027539.html