Patient Controlled Medical Records and eReferrals across Affinity Domains

February 11, 2005

Adrian Gropper
52 Marshall St.
Watertown MA 02472

This document and attachments are to be filed as a provisional patent application in advance of upcoming public disclosure. The descriptions in these disclosures relate to two previous provisional filings[1][2] but may also include material that supports new claims. These disclosures should not be used in a way that jeopardizes the effective dates of the original patents.

BACKGROUND

An Affinity Domain is commonly described as people and the information systems they employ that have agreed to policies in advance that address governance and operational structure, privacy, security, normalized patient identification and coded vocabularies. Although this kind of formal prearrangement is reasonable between institutions, it is inconvenient and unmanageable for individual patients (and even doctors) that want to deal with new entities and individuals that may not have pre-established an Affinity Domain relationship.

The methods described in the two referenced US Patent applications and the current disclosure are a practical solution to the problem an individual faces when trying to communicate private medical information to virtual strangers. As such, they are useful in electronic referrals – eReferrals – over the Internet.

A major benefit of the solution we describe is the separation of technology from policy. This enables a substantially uniform technology (MedCommons) to support a multiplicity of Affinity Domains with different policies and to be useful even to individuals who often make decisions about the Affinity Domains they trust on a case-by-case and day-by-day basis.

[1] U.S. Patent Application No. : 60/550,030 SYSTEM AND METHOD FOR PATIENT CONTROLLED COMMUNICATION OF DICOM PROTECTED HEALTH INFORMATION March 19, 2004 Gropper et al.
[2] US Patent Application No. 60/571,832 SYSTEM AND METHODFOR VIRTUAL RADIOLOGY AND PATIENT DOCUMENT FLOW May 17, 2004 Gropper et al.

OVERVIEW OF METHODS

The solution combines a central enterprise that is relatively policy neutral with technology accessible over the Internet that is accessible to enterprises that can agree to participate in a single affinity domain in advance as well to individuals (and other enterprises and affinity domains) that wish to interact with the established affinity domain.

The access technology, as previously described in the provisionals we reference is a gateway information system that is controlled by the host enterprise or user. Alternatively, the functions of this gateway are managed by use of a secure Web browser.

In the preferred embodiment, the access gateway is Open Source Software that may be more easily analyzed, trusted, and integrated into an enterprise's information systems and devices.

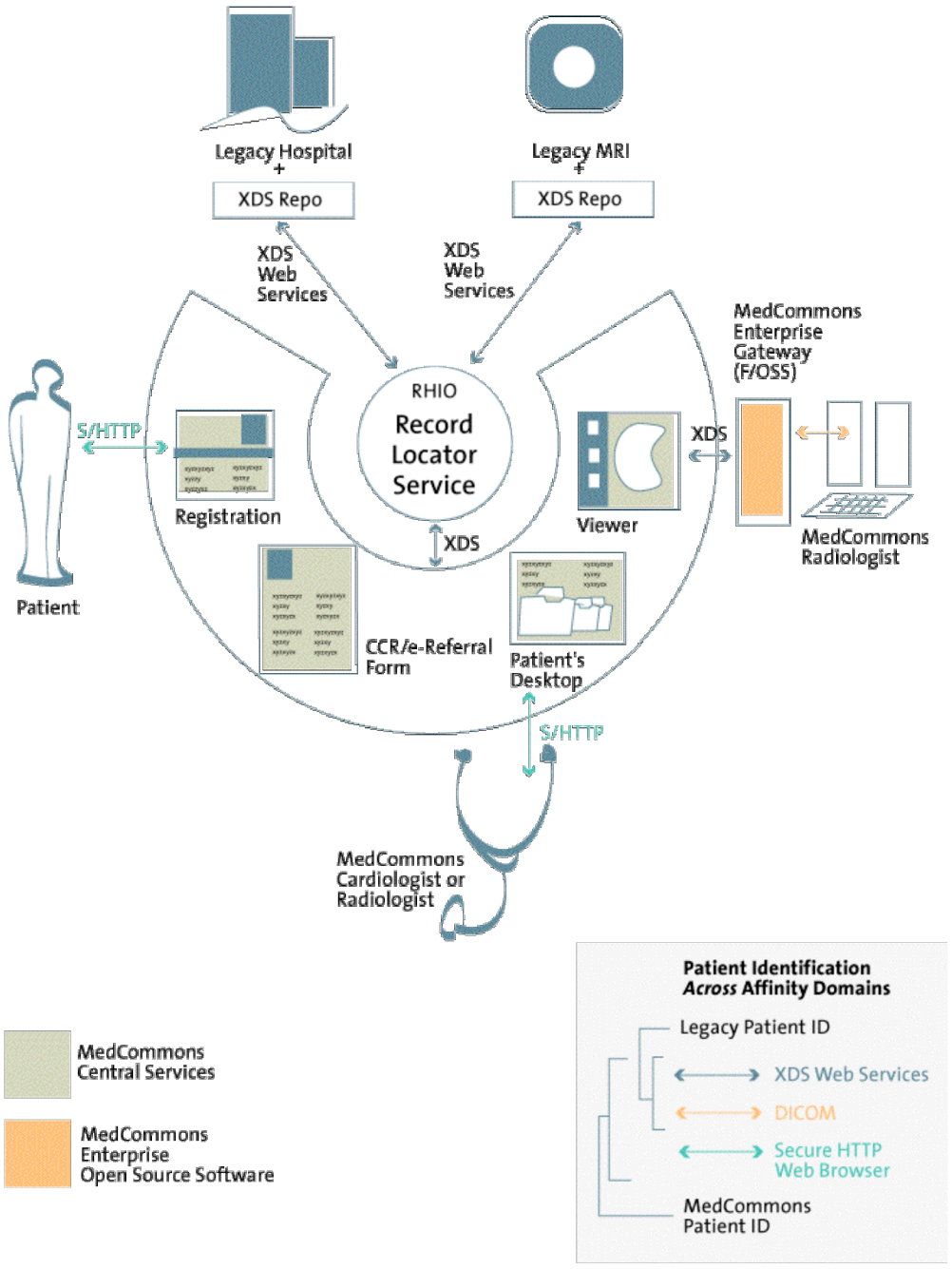
As previously described in the two provisionals, the Central System manages security and activity logs and encryption keys so as to provide a policy-neutral infrastructure for implementation of multiple affinity domains and interaction with individuals. For example, MedCommons has adopted IHE-XDS, ASTM-CCR and HIPAA as the affinity domain neutral foundation for technical interoperability and legal redress.

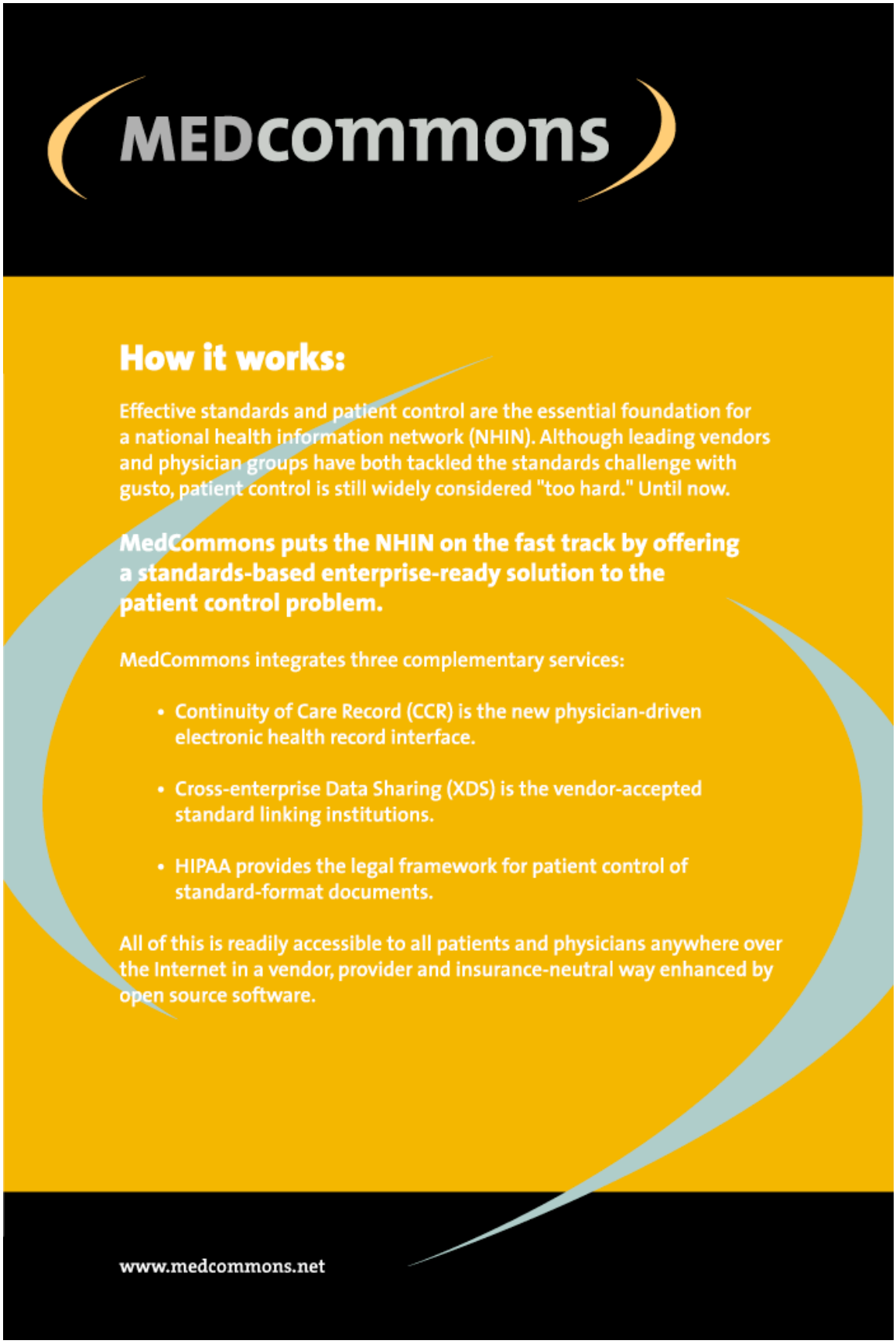
Two novel methods are claimed:

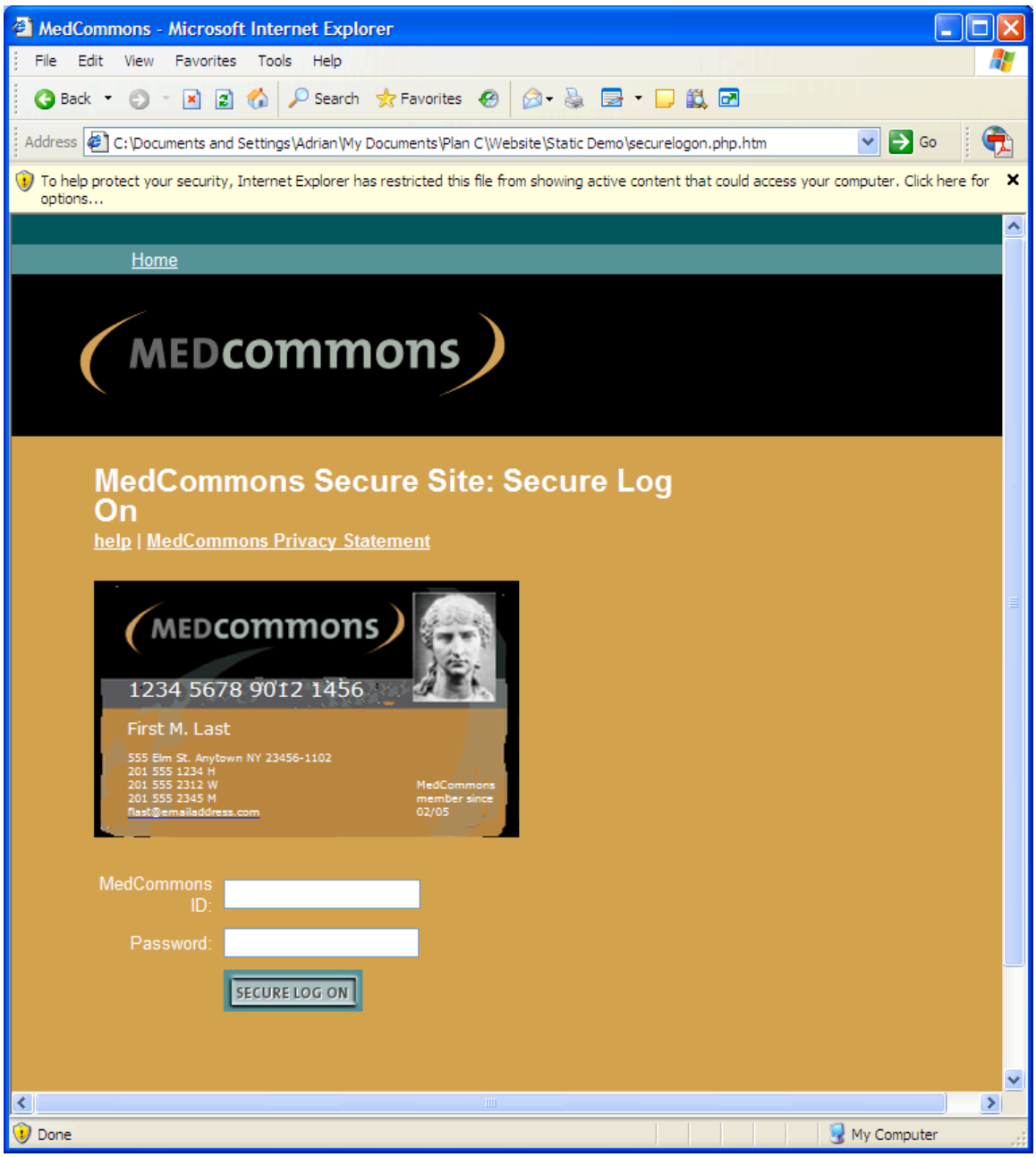
1 – To protect the user's privacy relative to medical information that have stored on behalf of an individual user, the central system offers users the option of verifying their own presence of the point when the information is requested from the central, policy-neutral repository service (MedCommons). One simple way to do this is to require use of a Debit Card to initiate the transaction disclosure or otherwise identify the presence of the individual at the point of use.

A related method to support trusted use of centrally stored information across multiple affinity domains under patient control is to provide a means for the patient to set and communicate a unique PIN number to the recipient in a manner that is complementary to the central system. For example, a telephone call directly between the patient and their intended user can communicate a PIN that allows access to information managed by the central system.

2 – To establish patient control while maintaining a policy neutral infrastructure, the central system allows patients to manage their own identity independent of any particular affinity domain. The central system ensures uniqueness of ID's but does not restrict the patient's choice of ID and when to use it. One simple way to do this is to provide the patient with technology and forms that allow them to request that a particular ID that hey control is linked or associated with their identity as known and controlled by an affinity domain. This innovation moves the problem of identity management and information aggregation away from the affinity domain and into the control of the patient. This then is the second method that allows the central system to provide a policy-neutral technical infrastructure.


Legacy Hospital
+
XDS Repo
Legacy MRI
+
XDS Repo
XDS
Web
Services
XDS
Web
Services
MedCommons
Enterprise
Gateway
(F/OSS)
RHIO
Record
Locator
Service
S/HTTP
Registration
XDS
Viewer
XDS
MedCommons
Radiologist
Patient
XDS
CCR/e-Referral
Form
Patient's
Desktop
S/HTTP
MedCommons
Cardiologist or
Radiologist
MedCommons
Central Services
MedCommons
Enterprise
Open Source Software
Patient Identification
Across Affinity Domains
Legacy Patient ID
XDS Web Services
DICOM
Secure HTTP
Web Browser
MedCommons
Patient ID


MEDcommons
How it works:
Effective standards and patient control are the essential foundation for a national health information network (NHIN). Although leading vendors and physician groups have both tackled the standards challenge with gusto, patient control is still widely considered "too hard." Until now.
MedCommons puts the NHIN on the fast track by offering a standards-based enterprise-ready solution to the patient control problem.
MedCommons integrates three complementary services:
• Continuity of Care Record (CCR) is the new physician-driven electronic health record interface.
• Cross-enterprise Data Sharing (XDS) is the vendor-accepted standard linking institutions.
• HIPAA provides the legal framework for patient control of standard-format documents.
All of this is readily accessible to all patients and physicians anywhere over the Internet in a vendor, provider and insurance-neutral way enhanced by open source software.
www.medcommons.net


MedCommons - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address C:\Documents and Settings\Adrian\My Documents\Plan C\Website\Static Demo\securelogon.php.htm
Go
To help protect your security, Internet Explorer has restricted this file from showing active content that could access your computer. Click here for options...
Home
MEDcommons
MedCommons Secure Site: Secure Log On
help | MedCommons Privacy Statement
MEDcommons
1234 5678 9012 1456
First M. Last
555 Elm St. Anytown NY 23456-1102
201 555 1234 H
201 555 2312 W
201 555 2345 M
flast@emailaddress.com
MedCommons member since 02/05
MedCommons ID:
Password:
SECURE LOG ON
Done
My Computer

MedCommons™ CCR / eReferral Form

Medical Center: _____

Patient Identification:

Name:

Date of Birth:

S.S.#:

Patient ID #:

Notifications

Send Email for:

[ ] Patient Notification

[ ] Recipient Notification

[ ] Recipient will also require direct patient contact for XDS* access to private health information.

[ ] Acknowledgment Email to Sender and Patient

HIPAA Patient Control Request

[**X**] Please include my **MedCommons Account ID 1234 5678 9012 3456** on all XDS Submissions

Signature of Patient _____ Date _____

*XDS is a technical interoperability specification that is currently the best practice for cross-enterprise data sharing. MedCommons(TM) is implementing XDS on behalf of this patient and to the benefit of the health care providers of the patient's choice.