MedCommons Privacy Policy
v0.2
Effective Date: February X, 2005.
DRAFT: This policy is released for public comment and is subject to change prior to the initiation of confidential patient services.

MedCommons has prepared this privacy statement to demonstrate our firm commitment to your privacy and your security as you visit and use the services provided by this site.

How we protect your privacy and your information.

1. MedCommons is committed to giving you, the patient, control over your medical data to the fullest extent permitted by law. Some of the ways we provide patient control include
   a. MedCommons uses the existing HIPAA privacy law as the foundation for patient control.
   b. MedCommons creates a modified HIPAA Restrictions Form to make it easy for the patient to request copies of certain standard documents from their health care providers.
   c. MedCommons interprets patient control to include the right to conveniently view, copy, store, add and remove health care-related documents before sharing them with the health care provider of your choice.
   d. MedCommons preserves your legal options and facilitates medical records interchange by maintaining the integrity of documents signed by your health care providers. You can, however, remove entire documents from referral folders prior to transmission to a health care provider.
   e. MedCommons does not alter the contents of your signed or unsigned health care documents in any way. You and your designated health care providers are the only parties that can see, add or remove documents from your account.
   f. MedCommons maintains secure logs of all account activity as required by law. This allows you, the patient to review which health care providers (individuals or enterprises) have viewed or added documents to your repository account.
   g. MedCommons will delete documents only with the patient's permission. Deletion activity is managed and logged as required by law.
   h. MedCommons will not review, aggregate, sell or divert a patient's private health information except as might be required by law.
   i. Although MedCommons employs encryption technology and formal security practices to protect patient privacy, patients may choose to further encrypt their private health information with keys that are not available to MedCommons at all. Such patient-controlled encryption is allowed by MedCommons but patients must acknowledge the increased risk of information loss and potential difficulty in emergency access if they choose to control their own encryption.

j. MedCommons cannot and does not maintain control of documents once they are passed to a health care provider or other destination designated by the patient. The MedCommons logs will not reflect any activity related to the documents once they are in the possession of the provider.

k. MedCommons can be used for provider-to-provider communications that do not directly involve the patient. These communications will be supported by MedCommons in a manner that preserves the accountability of the providers and the legal rights of the patient. The patient will be able to review the logs of such provider-to-provider communications of their personal and private health information. MedCommons may make copies of documents passed during provider-to-provider communications on behalf of the patient and store these copies automatically in the patient' repository account.

l. MedCommons can be used for provider-to-provider, provider-to-patient and patient-to-provider communications. Notification of the recipient that there are documents accessible to them can be made by MedCommons at the request of the patient or a provider authorized by the patient.. Notifications are considered insecure and MedCommons encourages users of the notification features to carefully check these communications for inadvertent private health information. MedCommons access restrictions and privacy policies apply to health care documents and not to the notification that documents might be available.

m. MedCommons will not release documents or any of the information contained therein unless explicitly requested by the patient or required by law.

n. Access to documents in the patient's repository account is managed by MedCommons on the patient's behalf. At the discretion of the sender, access to a document may be granted if the recipient is

    1. affiliated with an enterprise that the sender accepts as being trustworthy
    2. granted access by the patient in person
    3. granted access remotely by the sender through a direct communication of a password or PIN that is not known or accessible to MedCommons

2. The information that we collect while visiting this site is used
    a. To protect your account from unauthorized access
    b. For the processing of your requests and service to your account
    c. To improve and enhance our services to our customers

3. We use cookies to enhance the user's experience on our website. A cookie is a small file placed on your hard disk by a Web page server. Cookies cannot be used to run programs or deliver viruses to your computer. Most browsers are initially set to accept cookies. If you'd prefer, you can set yours to refuse cookies. However, it is likely that most areas of this site will not function properly if you do so.

4. This website makes links to other websites, however, MedCommons is not responsible for the privacy practices of those web sites. This MedCommons Privacy Policy applies solely to information provided by this website.

5. We will not and do not provide our client list to a third party..

The policies and practices described in this MedCommons Privacy Policy are subject to change. Any revisions to this MedCommons Privacy Policy will be posted 30 days prior to its effective date. Material changes will be prominently posted on the home page or by notification to registered users via email. We strongly encourage you to review this statement periodically. By using this site you acknowledge acceptance of this privacy statement at the time of use.

Registration and Verification of Patients and other Users who will be accessing PHI.

1. Users establish a Temporary ID which is, by default, their Email and assigned a 4-digit Temporary Password. This stage is actually optional and merely a convenience to people who want to demo or to start the registration process online. This part of the registration process could be done by a provider or family member on behalf of a luddite patient. Demos are designed to discourage the persistent storage of PHI other than Contact info. Users will be strongly encouraged to supply a photograph that will appear on their HIPAA Restrictions Form. This will make it less likely that someone can impersonate them when dealing with providers.
2. The patient begins the Verification process by acknowledging whatever we require as the MedCommons Terms of Use and agreeing to pay the Verification fee ($5). Their credit card is charged. This verifies that the Contact info matches the credit card info at least in terms of last name and address. People who can't use this methodbecause they don't have a suitable relative with a credit card will need to use the USPS Verification method.
3. The patient chooses whether they will be contacted by phone or mail and supplies all of the Required info. They are assigned a 16-digit MedCommons ID and a date. This information allows them to see and print their MedCommons Account ID Card. Until they are Venfied, the user can use either their Temporary ID (Email) or their MedCommons ID along with their Temporary Password to access their account. PHI is still not supported.
4. The patient who chooses phone is contacted by phone and asked to state their name and type in the temporary password into the telephone keys. It is assumed that the Credit Card prevented spoofing of the identity. Also, the Temporary Password was never sent in the clear. If the Temporary PW is correctly keyed, then the Verification is complete and the user is told that they will need to change their Password before they can use the account for online access to PHI. If the keying fails, the user must return to the Website to trigger another call.
5. A user who chooses USPS will be sent a new password in the mail. A credit card payment is not required but the Verification fee will need to be sent in by check or COD at the Post Office. The user is told that they will need to change their Password before they can use the account for online access to PHI. Users who do not link their MedCommons Account to a Credit Card will lose a measure of security because they will neeed to give providers a MedCommons Tracking number or their ID number.
6. At this point, the MedCommons ID will be recognized in on-line transactions and will appear on the patient's HIPAA Restrictions Form.

Use

1. Validated Patients can access their own Accounts by entering their Account ID and their Password.
2. Validated Patients can give their Provider IDs to XDS Registries via MedCommons. The XDS Registries and Repositiories will decide on whether to

return info based on Provider IDs or not based on what they think of MedCommons and whatever information the Patient chooses to disclose about themselves (via MedCommons). By default, MedCommons will make only the information visible on the Patient's ID Card visible to the XDS Registry. Even this amount of disclosure must be explicitly initiated by the Patient. If the Patient gets authorized to use their Patient ID at the XDS Registry, then MedCommons will automatically grab a copy of the documents and Register them under the Patient's MedCommons ID. The Provider's Patient ID will be kept as well but only for forensic reasons.

3. Validated Patients can give their MedCommons ID's to providers by handing them a HIPAA Restrictions Form. A generic version of this form is automatically provided by MedCommons to each Validated user. These forms can be customized and branded by providers by Registering with MedCommons for $??? or by installing a supported MedCommons Gateway. The form requires the provider, unless they explicitly decline, to tag all info submitted to any XDS registries with the patient's MedCommins ID. In the future, we might add the further restriction that an email or other notification be sent to MedCommons even if the information is sent to another XDS Repository.
4. Providers that have the patient's MedCommons ID cannot automatically get to a Patient's data. In many cases this will not be an issue because the provider will have their own preferred affinity domains and MedCommons may not be a part of that. In other cases, the patient will have provided whatever data they want the provider to have as part of the referral and there's no great reason to give a provider automatic access to more recent data (e.g: a patient may get three separate second opiniions in parallel). FInally, some patients will choose (or the law may mandate) that providers who somehow declare a life-threatening emergency can"break the glass" and look at MedCommons info without the patient's explicit permission.

Revocation

1. Users can revoke submission of information to their Accounts by changing their MedCommons Account ID. MedCommons will associate the old and new Account IDs but this is not to be done lightly because it messes with the integrity of our system. Account ID changes are subject to a new Validation charge or worse. Loss of password is subject to a new Validation charge as well and may even require a notarized afidavit or some other extraordinary process.
2. Users who'se credit cards are compromised or expire will have to associate another credit card with their Account ID before they can view newly added information. Old info remains accessible.
3. Users and MedCommons can stop dong business with each other at any time on short notice. MedCommons will have aready mail a copy of the user's information to their address of record or will mail it prior to closing the account.
4. It is the user's choice as to whether MedCommons keeps information in the clear and mails it to them in the clear. Users that want to protect documents with a sepatrate password before uploading it to MedCommons can do so. Documents

will be returned to the user encrypted and the user will have to deal with decryption. WinZip, for example can be used for this purpose without MedCommons involvement or sanction but S/MIME or some other standards based mechanisms may be explicitly supported in future releases. Users who want to apply a password to a document already in MedCommons will be able to do so in future releases subject to the deletion provisions below.

5. Users can ask MedCommons to delete a document and we will comply to the extent allowed by law. All links to the document will be removed. A log will be kept of the deletion and the GUID of the document will be added to a deletion (revocation) list so that users that have saved the actual GUID will not be able to access the document directly without risking an alarm. In most cases, deletion of the actual document may not be guaranteed becouse some copies may be off-line or because some signed legal document s refer to the document and it's destruction is prohibited by law.

XDS Strategy Thoughts

- MedCommons business is eReferral within a RHIO-compatible infrastructure
    - eReferrals are accessible to Patients (Patient Portal value to the enterprise)
    - eReferrals are directed at providers with and without Gateways (Transfer value)
        - CCR – only transfers will be common
        - CDA and PDF will be used for reports
        - DICOM transfers will be a minority
        - Notification and Acknowledgement are key
        - XDS Standard adds value when there's an EMR at either end
- Enterprise Gateways are a free XDS Repository that is not tied to any particular Registry
- MedCommons Central is the default XDS Registry, but
    - A RHIO is encouraged to operate its own XDS Registry (licensed from MedCommons or not)
- The simplest eReferral transaction is editing of a CCR using the WADO Viewer or a thick client application (EMR).
    - If a thick client application generates the CCR, the user will drag&drop the document to create a new WADO Viewer Order
        - Document upload to MedCommons XDS Repository Gateway over SSL
        - If the document is a PDF or CDA, then the CCR is generated at MedCommons
        - Document encrypted for storage (Key exchange with MedCommons Central. Note that there is no Enterprise Gateway to use for encryption.)
        - Document registered in XDS Registry (MedCommons or RHIO)
        - This is new functionality that will appeal to physicians without an EMR but access to a CCR editor such as Dictaphone.
    - If the CCR is created in MedCommons
        - Document is encrypted for storage
        - Document registered in XDS Registry (MedCommons or RHIO)
    - If the document is DICOM
        - There's an enterprise Gateway involved and available for encryption
        - A CCR is automatically created by MedCommons
        - The documents are registered in XDS Registry (MedCommons or RHIO)
        - If a CCR is Registered for the same patient it replaces the automatically generated CCR (Sean to review this bit of XDS functionality).
-
- MedCommons Central tracks XDS Repository submissions via x509 Patient Certificates
    - MedCommons will add these to the documents if XDS does not support them (yet)
    - A patient or clinician user has One MedCommons ID at a time.
        - This ID is based on Registration and looks like a Plaxo business card with logo.
        - It is associated with a PKI Cert. issued by MedCommons or Verisign. The logo changes accordingly.
        - A Patient logs in with their pass phrase and can send their stuff already in MedCommons to anywhere with the MedCommons invitation mechanism.
    - A Clinician with passphrase can establish a temporary / proxy credential into IE or FF (just like gmail) and send CCR, PDF, CDA via MedCommons as above.
        - The Patient's ID (Business Card) will be displayed by MedCommons if possible.
        - If the Patient has not registered with MedCommons and does not have a Public Key on file with the clinician from somewhere else, then MedCommons will complain and proceed with the transaction anyway.
        - MedCommons will XDS Register the transaction with the local RHIO using the Patient's MedCommons ID.

- A Clinician with passphrase can establish a temporary / proxy credential into a MedCommons Enterprise Gateway and it will automatically create MedCommons CCR folders bared on DICOM, attach the Patient Public Key and proceed the same as a browser – only transaction above.
- A Clinician with passphrase can establish a temporary / proxy credential into a MedCommons Enterprise Gateway and it will automatically accept MedCommons CCR Folders across a firewall and decrypt them as they come in. Their MedCommons ID will be used in the MedCommons HIPAA log.
    - When their proxy expires, they will need to enter their pass phrase again.
- Certain operations like signing a CCR Report may require the paraphrase even if the proxy has not expired yet.

Requirements and Terminology

1. **MedCommons Gateways** are XDS-Repository standard with a built-in XDS Document Creator.
    a. The XDS Repository part is not externally available yet pending IHE certification. This is not a problem because there are very few XDS Repository clients out there yet. Dictaphone, I believe, took the same tack at this year's connectathon.
2. The **XDS Document Creator** component of our Gateways is the MedCommons CCR Folder Viewer (formerly known as the WADO Viewer). This year, our Document Creator handles CCR, CDA, PDF and DICOM from various sources on an enterprise LAN. If a CCR is not part of a MedCommons CCR Folder, then MedCommons creates one from DICOM or other metadata automatically.
3. The **MedCommons CCR Folder Viewer** is a patient-centric thing that never shows more than one patient. Multiple folders for a patient are shown as a CCR Folder Stack of dated folder with thumbnails for documents and one folder cover visible at a time on top.
    a. A CCR Folder Stack can result from an XDS Registry Query after a patient or clinician user logs into MedCommons. The XDS Registry will typically not be controlled by MedCommons – this is where the RHIO may come in.
        i. A Login to MedCommons Central (on the WAN) uses the MedCommons enterprise as the affinity group member to query the XDS Registry.
        ii. A Login to an Enterprise Gateway (on the LAN) uses that enterprise as the affinity group member to query the XDS Registry.
    b. The CCR Folder Stack and the MedCommons XDS Document Viewer are always one click away from each other.
4. Gateways have an **Encryption Flag**. It is typically off for Enterprise Gateways and enabled for Repository Gateways.
5. Gateways can have an optional **Verisign SSL Certificate**. This will typically be the case for Repository Gateways but could also be the case for Gateways that are placed in a DMZ by an enterprise. Note the little e – I suggest we treat Enterprise gateways as pure LAN entities. DMZ Gateways will not be considered any further for now.
6. MedCommons can act as an XDS Document Creator and a MedCommons CCR Folder creator on behalf of the Patient or a clinician. **No Enterprise Gateway is involved** because there is no enterprise other than MedCommons.