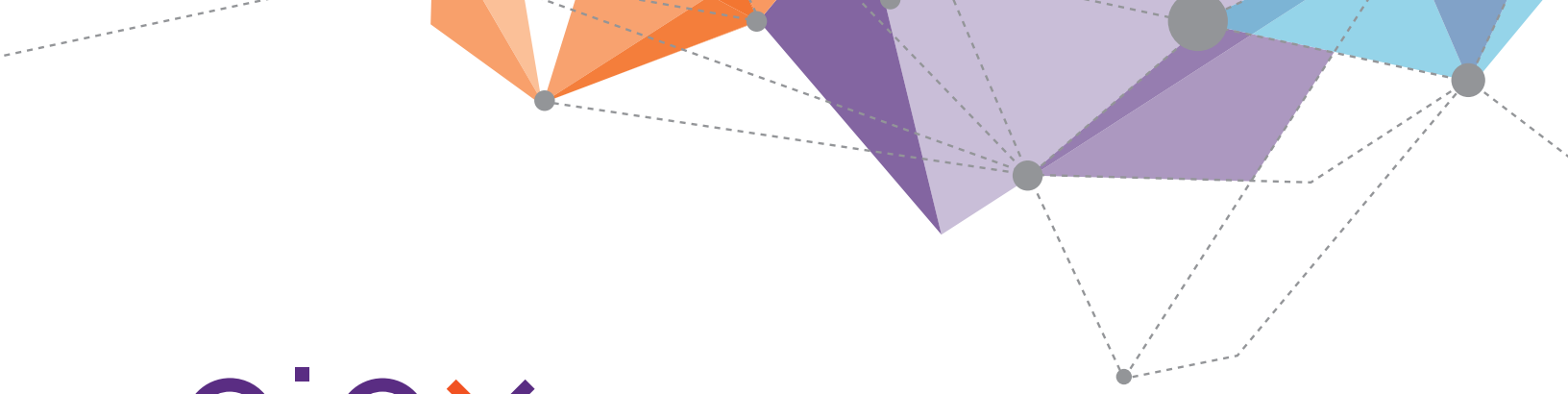


CIOX HEALTH

Remote Release of Information: The Next Step in Secure and Compliant Exchange of PHI

October 2016

First published August, 2016 Journal of AHIMA

Overview

Across the industry, HIM departments and medical groups are moving their health information management operations from hospital main campuses and individual physician practice sites to centralized, offsite locations to make better use of valuable square footage in their facilities. Paired with the continued adoption of electronic health records (EHR), HIM directors and practice administrators are leveraging this opportunity to reorganize and form 'virtual medical records' departments. Additionally, outsourcing of functions such as release of information allow the HIM staff to focus on other priorities of data governance while maximizing available space.

Costs associated with regulations, staffing, printing, mailing, and square footage are increasing; and in some instances, volumes of requests are increasing due to audits, lawsuits and the portability of healthcare. Furthermore, allowable fees for releasing medical records are decreasing in some states. With these negative financial pressures, healthcare providers will find it more difficult to make release of information a profit center in their organizations.

With the advent of Meaningful Use requirements and the increase in various governmental and payor audits, timeliness of response to request for medical records is critical and penalties for non-compliance are steep.

The results of a recent American Hospital Association survey entitled American Hospital Association Survey Results Summary on Hospital's Ability to Meet Meaningful Use Requirements of Medicare and Medicaid EHR Incentive Programs in January 2011 indicated that 95% of hospitals plan to meet Meaningful Use requirements while CMS reported that as of May 2011, 56,000 physicians had registered for Meaningful Use programs. On the audit front, takebacks from Recovery Audit Contractor (RAC) audits almost doubled from the last (calendar) quarter of 2010 to the first (calendar) quarter of 2011.

Healthcare providers are reaching the point of diminishing returns in regards to managing the release of information function on their own, and in some cases, will not be able to meet the time deadlines imposed upon them to gain incentives, avoid penalties and takebacks.

These new industry influences create the need for even faster, more efficient, error-free fulfillment of medical record requests.

The Remote Release of Information Process

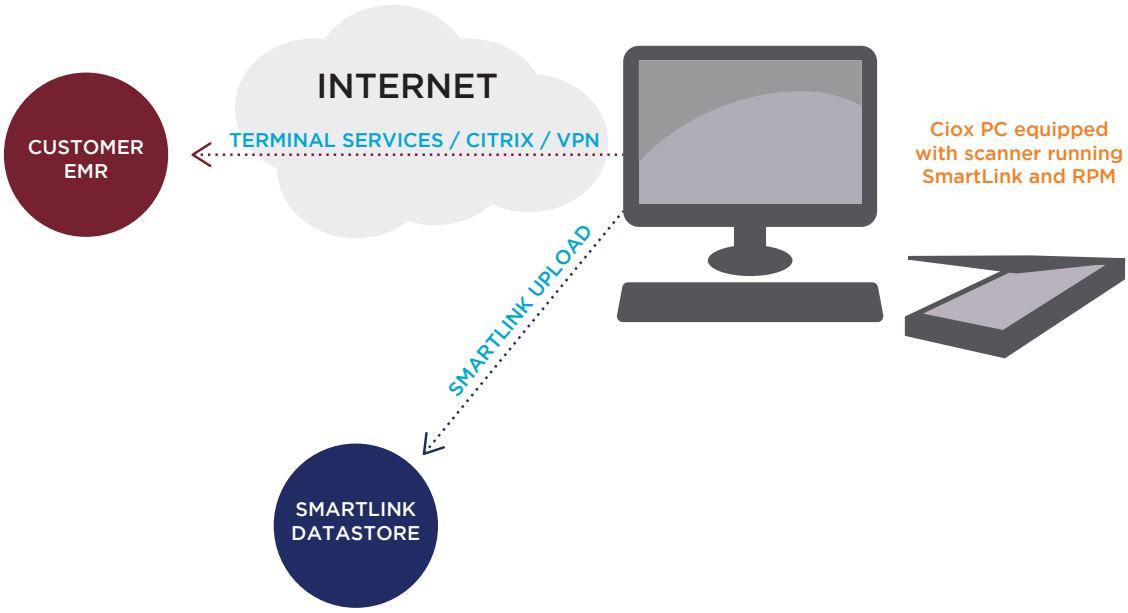
The release of information (ROI) process is a time-consuming administrative challenge for health information management professionals requiring compliance expertise, secure and efficient technology, as well as trained and knowledgeable staff.

The ROI process starts at the healthcare facility when requests for release of health information are received.

With Remote ROI, CIOX Health receives the request from the hospital or practice via a mutually agreed upon, secure mechanism. Securely connected and able to access the hospital or practice electronic health record, the Remote ROI Specialist reviews the requests for proper authorizations, identifies and captures the records to be released, and

transmits the medical records from the facility's EHR in an encrypted electronic format to CIOX Health's Remote ROI centralized processing center. The release is delivered to the requestor through an automatic print and mail process that excludes almost all human intervention or electronically via a secured website selected by the requestor clients.

By moving some or all of the onsite Remote ROI functions to an offsite secure centralized processing center, Remote ROI streamlines the ROI workflow and allows hospitals and physician practices to reclaim square footage for other purposes. Additionally, the immediate access to requests and authorizations speeds turnaround times on processing requests which is particularly important when considering tight timelines for Meaningful Use and audit-related releases.



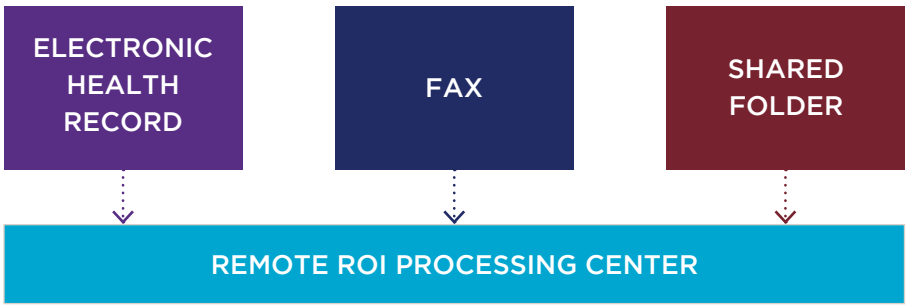
Four fundamental steps establish the workflow for successful Remote ROI:

1. Determine the method of access to the Request Letter/Authorization received by the hospital or physician practice.
2. Establish connectivity to the EHR to validate the authorization, review the medical records, and process the request.
3. Configure document capture technology for secure capture and transmission of medical record information from the
4. facility's EHR to the centralized processing center for distribution.
5. Ensure compliance standards to track when and who accessed protected health information.

Determine Method of Access to the Requests Letter/Authorizations

There are several mechanisms by which requests and authorizations are securely made available to the Remote ROI Specialists for release of information processing. The following are the most common methods:

- Requests/Authorizations are scanned into the EHR – Staff at the facility scans the requests/authorization into the EHR. The Remote ROI Specialist accesses the EHR remotely to view the information and begin the process.
- Requests/Authorizations are faxed – Staff at the facility faxes the requests/authorizations to a fax-in queue provided by CIOX Health. The Remote ROI Specialist accesses the fax-in queue to view the information. When the requests are processed by CIOX Health, the requests/authorization will be available for viewing through CIOX Health's web-based logging and tracking application, eSmartlog.
- Requests/Authorization are scanned and placed in a shared folder – Staff at the facility scans the requests/authorization into a shared folder accessible by the Remote ROI Specialist at the secure CIOX Health Remote ROI Processing Center.



Establish Connectivity to the EHR

CIOX Health makes the security of the exchange of protected health information a top priority. An acceptable baseline for securing the connection to your EHR system(s) must be established for Remote ROI. Distinct and necessary remote access requirements have been identified to securely access your facility's EHR. The appropriate connectivity scenario depends on the underlying technologies at your facility. This section explores the different technologies and the requirements that will provide the adequate baseline for securing the connection to your systems.

Connectivity options include:

EHR Web- Interface

If your EHR supports functionality using a web-based interface AND your security policy will allow exposure of that webinterface over the Internet, this model meets the acceptable security standard given the following assumptions:

- 2048-bit signed 256-bit AES (or greater) Secure Sockets Layer (SSL) security is implemented
- A password policy is implemented that meets or exceeds the HealthPort corporate standard

Remote Virtual Private Network (VPN)
If your facility has an existing method for providing secure remote access to your enterprise network, extension of this capability will be acceptable given the following assumptions:

The VPN uses Internet Protocol Security (IPsec) standards, leveraging at least 256-bit AES encryption
OR
An SSLVPN implementation which uses at least a 2048-bit key size and
256-bit AES (or greater) cryptographic module
AND
Either strong authentication (token) OR an acceptable password policy

Other Commercially Supported Remote Access Solution
If your organization leverages a remote access capability that is delivered as a service such as GOTO My PC, provisioning and use of an account will meet the standard provided the following assumptions are followed:

- The connection leverages a 2048-bit key size and 256-bit AES (or greater) cryptographic module
- No data is stored or decrypted on the provider systems
- Validation that keystroke and/or session logging is not possible in any client/server components of the solution

Remote Desktop Services (Terminal Services)
If your hospital or practice utilizes remote desktop functionality to enable access to the EHR, this will meet the standard provided the following assumptions are followed:

- Transport Layer Security is implemented to encrypt the connection using a minimum 256-bit cryptographic module
- A password policy that meets the CIOX Health Password Policy is enforced
- The platform is Windows Server 2003 or later

Configure Document Capture Technology for Secure Transmission

SmartLink is HealthPort's EHR document capture system. It ensures the complete security of the link between your electronic health record and CIOX Health's Release of Information system. SmartLink

is a client-server based application and requires a Windows PC for operation.

Heading
Subheading
Insert text here.

When configuring systems and connections for Remote ROI, typically the standard installation of SmartLink is on CIOX Health's local PC, and the EHR documents are accessed from the PC to the facilities via the encrypted connection outlined above. The copies of the electronic documents are then captured and transmitted across the encrypted connection to HealthPort's secure Remote ROI processing center for fulfillment.

If required by your facility and you are using a remote server connection such as Citrix or RDP, SmartLink can also be installed on the facility's server and accessed remotely through the encrypted connection. This configuration will package and encrypt the records first before being transmitted to CIOX Health's secure Remote ROI processing center.

Operational functionality of SmartLink varies little whether it is installed on the local facilities remote controlled server or CIOX Health's PC.

Ensuring Compliance Standards (Password and Access Management)

PCs located at CIOX Health's Remote ROI processing facility are secured utilizing Symantec's End Point Disk Encryption, Anti-Virus Protection, and Web Filters.

Passwords provided by the facility for access to their specific electronic health record are stored in an electronic password vault. This password vault is linked to CIOX Health's Active Directory and can only be accessed by the ROI Specialist using their Active Directory account. The Active Directory account adheres to the password guidelines established in the CIOX Health Password Management Policy. This policy includes password strength, age, and expiration. Usernames and passwords are unique to each user.

If used, secondary authentication devices such as access tokens are stored in a locked box and access is controlled by Operations Management.

CIOX Health provides complete audit trail capabilities to track personnel accessing your electronic health record and processing medical record requests from your applications.

Getting Started: Implementation Steps

Beginning Remote ROI service is typically quick and easy. There are eight steps from the signing of the agreement to the start of remote request processing:

1. Sign Remote ROI Agreement and /or Service Addendum.
2. Participate in an initial implementation call with CIOX Health Remote ROI Team, CIOX Health OPS Manager, and your site's IT personnel and site manager to discuss request/authorization access, connectivity, and project schedule.
3. A Remote ROI Specialist is assigned to your site.
4. Connectivity, SmartLink configurations and user credentials are established.
5. Unique Site Process Protocol is completed which communicates site-specific requirements related to release of information protocols.

6. Your Remote ROI Specialist is trained on the Unique Site Process Protocol. Training for the site's electronic health record system is conducted.
7. CIOX Health begins processing requests.
8. CIOX Health provides ongoing support and reporting to the site.

Customizing the Remote ROI Experience to Meet Each Customer's Needs

Hospitals and physician practices have varying protocols and processing guidelines for handling release of information. Certain restrictions and considerations are documented and followed for each individual site to provide a seamless transition from onsite to remote processing. These restrictions and variations may include, but are not limited to, instructions on how to manage:

1. Special requests from patients, audit requests, Meaningful Use requests, or other special requests.
2. Accounting of Disclosures
3. Records that your ROI Specialist must NEVER SEND
4. Documentation of non-billable requests
5. Questions about specific processing requests
6. Certified records

Transparency into Remote Release of Information Activity

Requests are entered and information is available at any time through HealthPort's web-based logging and tracking tool, eSmartlog. HealthPort's Remote ROI reporting also includes:

- Productivity and turnaround times
- Request Status
- Invoice Information
- Accounting of Disclosures
- Custom Reporting

CIOX Health Remote ROI Services

Flexible Remote ROI service delivery levels available through CIOX Health include:

Remote ROI – In this scenario, your hospital or physician practice currently operates solely with an electronic health record and provides secure, remote access to your system. This connectivity allows HealthPort to manage the entire release of information process from the CIOX Health Remote ROI processing center in Alpharetta, GA. This service level includes:

- Request capture and authorizations
- Request logging and tracking
- Chart retrieval
- Document capture and validation
- Printing and packaging
- Mailing or eDelivery of requests
- Billing and collections
- Ongoing management relationship with local District Manager

Remote ROI Plus – For the Remote ROI Plus service level, the hospital or physician practice maintains some paper medical records while operating primarily with an electronic health record. CIOX Health provides onsite services as needed by the facility. This service level includes:

- Customer service functions
- Request capture and authorizations
- Request logging and tracking
- Chart retrieval
- Document capture and validation
- Printing and packaging
- Mailing or eDelivery of requests
- Billing and collections
- Ongoing management relationship with local Manager

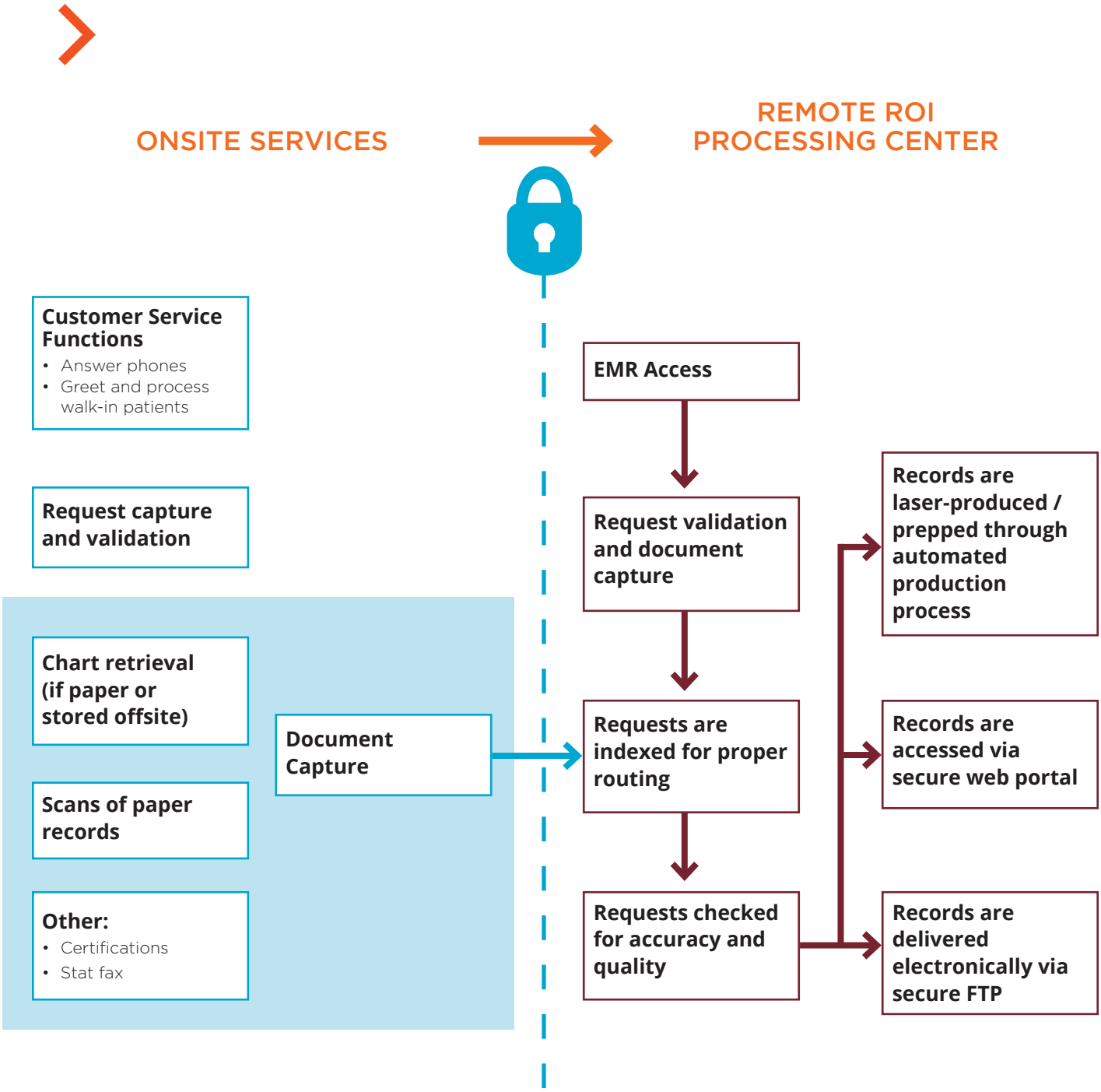
For more information about CIOX Health's Remote ROI services or our other flexible service levels including Onsite ROI and ROI Partner, please contact a CIOX Health representative.

(graphic)Ongoing management relationship with local District Manager

Remote ROI Plus – For the Remote ROI Plus service level, the hospital or physician practice maintains some paper medical records while operating primarily with an electronic health record. CIOX Health provides onsite services as needed by the facility. This service level includes:

- Customer service functions
- Request capture and authorizations
- Request logging and tracking
- Chart retrieval
- Document capture and validation
- Printing and packaging
- Mailing or eDelivery of requests
- Billing and collections
- Ongoing management relationship with local Manager

For more information about CIOX Health's Remote ROI services or our other flexible service levels including Onsite ROI and ROI Partner, please contact a CIOX Health representative.



925 North Point Parkway, Suite 350
Alpharetta, GA 30005

cioxhealth.com