



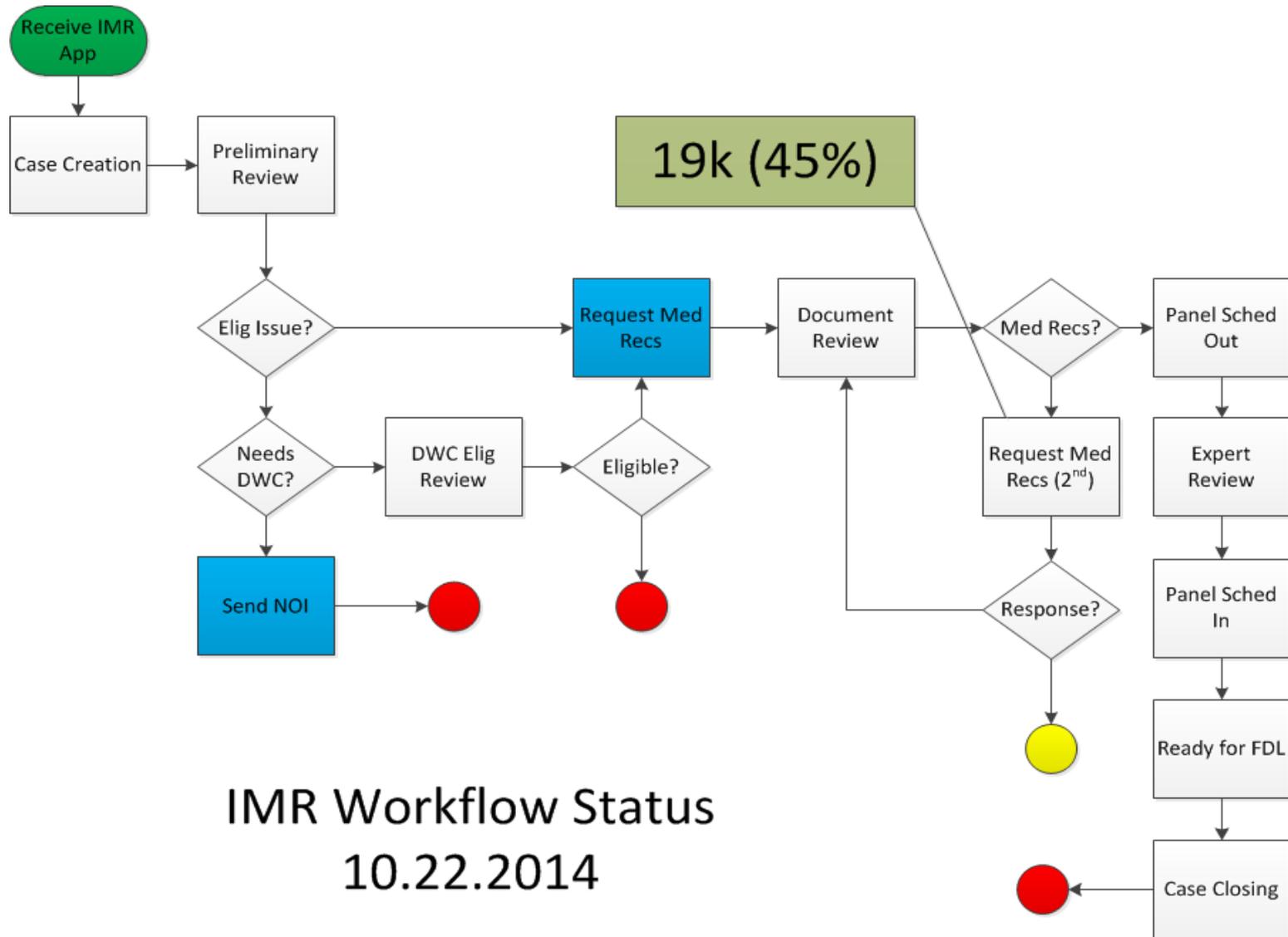
IMR: Submitting medical records Electronically October 22, 2014

- **MAXIMUS Federal Services (MFS)**
 - Lou Shields – Project Director, IMR and IBR
 - Rob Nydam – Project Manager, IMR
 - David Nunn – Technical Project Lead, IMR
 - Steve Marschall – Senior Manager, EDI Services

Purpose

- To discuss technical options for exchanging medical records electronically with MFS
- To make the process of submitting medical records easier :
 - Secure
 - Traceable
 - Auditable

IMR Today



- Of the 42K open IMR's, 19K are missing medical records past the deadline for submission
- Of those 19K, roughly 80% had a NOARFI sent on or after June 1, 2014
- Conclusion: when we cleared our backlog, it created backlogs for you
- We need to work together to clear these backlogs once and for all

Submitting medical records: things to keep in mind

- Best bet: use MOVEit (more on this later)
- Next best: facsimile
- Worst: USPS/Fedex/UPS
- Also – if submitting records for multiple cases at the same time, please make sure records for each case are clearly marked/separated.
 - Recommendation: use barcoded sheet from NOARFI

Recent addition of barcodes with NOARFI

PDF file.

MAXIMUS FEDERAL SERVICES, INC.
Independent Medical Review
P.O. Box 138009
Sacramento, CA 95813-8009
(855) 865-8873 Fax: (916) 605-4270



MAXIMUS Case Number:



CM14-555555

Document Type Requested:



Medical Records

Participant:



Injured Worker

Security Overview

- MFS provides IT services and supportive systems to a wide variety of state health and human services, child welfare, financial and administrative agencies as well as for the Federal Government.
- Continuously audited by our state and federal clients. In addition, we contract for our own external AICPA SOC 2 and SOC 3 audits of our data centers.
- MFS follows standard security practices as outlined in the NIST Special Publication 800-53 moderate risk controls.
- The MOVEit system is currently deployed in another CA project. This program has been in place for several years and is tracked and monitored by DHCS and ultimately the Governor of California's office. Data is encrypted in transit and at rest using FIPS 140-2 certified encryption.

MOVEit Security continued

- sFTP communication to Portal as well as HTTPs to Portal follows secure transfer model
- sFTP is ID/pswd & Key exchange driven
- MOVEit is FIPS 140-2 Certified by the Federal Government
 - for data at rest
 - for data in-transit
- All major Browsers supported
- Windows installer .msi available for distributed install
- PGP Encryption can also be used for added layer of security

MOVEit Options for Claims Administrators

- MFS can work with you in 3 comprehensive & simple ways each in a secure fashion :
 1. Automated SFTP from CA IT organization into/out MOVEit as required
 2. Automated SFTP from MFS to CA's Server as required
 3. Secure SSL/TLS Self Service Web Portal with upload/download capabilities upon customer initiated logins (smaller IT Organizations without automated file transfer capabilities)

File Naming & Type Standardization

- Standard file type: All file types must be PDF's
- One CASE per file/PDF (can be multiple pages, but one PDF per Case)
- Standard naming convention including MFS Case ## (CM13-xxxxxx or CM14-xxxxxx) for each PDF file
 - Expedites connection between Case Management system and Document management system
- If CA doesn't have the ability to combine PDF's, then naming convention can add file number for same case numbers (ie CM13-123456-001, CM13-123456-002.....etc.....)

OPTION 1

- **Option 1 – Our preferred method**

Mature CA IT Organization takes full control of their file transfers and sets up automation to push and pull files from MFS Secure File Transfer Server. Usually volume driven

Steps:

1. CA IT Organization contacts MFS Liaison to begin the process
2. MFS exchanges a File Transfer Access Sheet from CA
3. MFS ID/Pswd is setup to begin testing
4. Keys exchanged to more securely exchange information in phase 2 of testing
5. CA IT Organization sets up Automation of their delivery and pick-up of files
6. File schedules exchanged

Option 1: SFTP to MFS is working well

- We have 10 CA partners setup for SFTP and working well
- Process takes 1-2 weeks depending on IT organization involvement and testing efforts

- **Option 2 – Our 2nd Choice, but still Automated**

MFS takes control of file transfers and sets up automation to push and pull files from Maximus' Secure File Transfer Server

Steps:

1. MFS contacts CA IT Organization Liaison to begin the process
2. CA IT Organization ID/Pswd is setup to begin testing
3. Keys exchanged to more securely exchange information phase 2 testing
4. MFS sets up Automation of their delivery and pick-up of files
5. File schedules exchanged

Option 2: SFTP from MFS

- We currently have no Claim Admin groups working with Option 2
- Majority of IT orgs like to do option 1, not 2....
- MFS preference is Option 1 where CA's control their own file transfers and schedule themselves

OPTION 3

- **Option 3 – Self Service Web Portal**

This option is generally for smaller CA's without a large IT organization and no real file transfer server. Using this self serve option CA users can manually download and upload files on demand.

Steps:

1. CA contacts MFS Liaison to begin the process
2. MFS registers CA emails for self registration on MOVEit Web Portal
3. MFS provides user MOVEit user guide to CA's
4. CA registers email/s on Web Portal and begins testing directory movement and upload/downloads
5. CA determines comfort with process and begins use at own pace

Option 3: MOVEit Self Service Secure Web Portal

- We currently have 29 CA's setup with well over 100 user ID's
- Individual and multi file upload/downloads via browser interface
- User feedback has been outstanding

Option 3: IMR Directory structures

IMR MOVEit Directory structures:

- CA-NAME\from_Max
 - Files from MFS to the CA
- CA-NAME\to_Max
 - Files from the CA to MFS

Option 3: MOVEit Browser Encryption Settings

Encryption Settings must first be set in the browser/s you will use to exchange files with MOVEit

- TLS 1.0 must be set in Options
- Must set the MFS Secure Xchange Portal as a “TRUSTED SITE” (<https://xchange.maximus.com>)

* May need IT Organization Support

Option 3: MOVEit Upload/Download Wizard Installation

- In addition to security settings in the browser there is an Upload/Download Wizard provided by MOVEit that is a GREAT feature
 - Offers faster upload/download than browser built-in functions using compression on the fly
 - Shows active status bar for transfers
 - Provides integrity checking upon completion to ensure files are the same at both locations

Option 3: MOVEit Demo

- Now we would like to do a demo of the setup steps and use of MOVEit for the CA's that will use it

Demo includes:

1. Security Setup in Browser (TLS & Trusted Site)
2. UserID Registration & Sign-on
3. Upload/Download Wizard
4. Overall Navigation to folders
5. File Upload & Downloads

OPTION 3: MOVEit Live Demo

Claims Administrator's Next Steps

- Review 3 options with your management and IT staff for best choice for your situation
- Contact MFS (IMRFILETRANSFER@MAXIMUS.COM) and inform them of decision on options OR with any questions or needs to make your decision
- Test, Test and re-Test
- Start using Option of choice once agreed upon with CA and MFS that you are ready!!!!

- **Resource Documents to be provided By MFS**
 - CA Options for File Transfer
 - MFT Access Sheet (Only for Option 1 & 2)
 - MOVEit Xchange User Guide (Option 3)
- Additional Vendor Information for reference from Ipswitch:
 - MOVEit DMZ Protocols in place to ensure Security of files
 - What internal expertise, tools and procedures do you use to ensure MOVEit software is extremely secure?