NEW YORK STATE | Department of Health | Medicaid Redesign Team

Data Security & Information Sharing

A review of the requirements and necessary steps to secure access to DOH provided Medicaid PHI data, and the impact of opt-out on information sharing outside of the Medicaid Analytics Performance Portal (MAPP).

July 2015

Webinar Overview

Data Security Introduction

- Need for Improved Security Controls

Controls for Accessing and Sharing Data

- Relevant Policies and Standards for Data Security
- Processes and Controls for Accessing and Sharing DOH Medicaid Data
- Secure File Transfer Process
- What’s New in MAPP: Two-Factor Authentication (2FA)

Opt-Out Process and Long Term Data Sharing

- Timeline of PHI Data Release
- Longer Term Data Sharing Tasks
- DSRIP Opt-out Letter
- About the DSRIP Opt-Out Process
- Destruction of Data and Sharing Post Opt-Out

Data Security Requirements – Importance

Jonathan Halvorson, Office of Health Insurance Programs, Director of Systems

Recent National Breaches

Breach	Description	# Records	Suspected Root Causes
Anthem	Criminal attackers obtained data from compromised servers. Stolen data will likely be sold on black market and used for Phishing attacks on individuals.	80 M	State sponsored attack suspected, Phishing, fake domains "*we11point.com*". Lack of awareness.
Federal Office of Personal Services	One of the largest breaches of federal employee data. Personal information and security clearance data stolen. Undetected for a year. Hackers obtained administrative permissions.	18 M	State sponsored attack, zero-day tool against existing vulnerability. Sensitive data stored unprotected.
Premera Healthcare	Company breached and then slow to respond and is now being sued by 5 groups.	11 M	Malware on systems, insufficient controls
Carefirst	Initial breach discovered last year, company assumed it was resolved; however, 10 months later data was still being lost.	1.1 M	Lack of awareness to Phishing attacks

HIPAA Breach Penalties

Violation	Amount ***per*** violation	Max for violations of an identical provision in a calendar year
Did Not Know	$100 - $50,000	$1,500,000
Reasonable Cause	$1,000 - $50,000	$1,500,000
Willful Neglect — Corrected	$10,000 - $50,000	$1,500,000
Willful Neglect — Not Corrected	$50,000	$1,500,000

Healthcare Related Breaches & Trends

- Premeditated criminal attacks are the new leading cause of data breaches in healthcare
- According to the Washington Post and CMS since 2009
  - Data about more than 120 million people has been compromised in more than 1,100 separate breaches at organizations handling protected health data.
- Healthcare data is being targeted because it has a long shelf life compared to credit card data where new cards are re-issued after a breach, individual's private data losses cannot be so easily repaired.

Relevant Policies and Standards for Data Security For Non-MAPP Access to DOH Medicaid Data

Rob Zeglen & Vince Hannon- NYSTEC

NYS Identity Assurance Policy NYS-P10-006

What it is

- Outlines steps and provides worksheet for completion of an Identity Assurance Assessment

Relevance to DSRIP

- Part of the security assessment process to enable remote access to DOH Medicaid data

How it works

- Identifies information owners and assembles the assessment team
- Gathers system information
- Identifies user roles
- Determines Assurance Level for each user

What you need to do

- Use the procedure in the policy to determine the Identity Assurance Level for users who will be accessing DOH-provided Medicaid data.

NYS Identity Assurance Standard NYS-S13-004

What it is

- Outlines requirements for identity-proofing and account-management, according to Identity Assurance Level (IAL)

Relevance to DSRIP

- Identifies security controls by IAL, necessary to enable remote access to DOH Medicaid data

How it works

- IAL 3 includes requirements, such as:
  - In-person identity proofing using a government/employer-issued ID and validation with issuer.
  - Two-factor authentication for accessing ePHI, including DOH Medicaid data
  - For the full list of requirements, consult NYS-S13-004.

What you need to do

- Follow standard to validate users, and manager accounts during initial account set-up and for support requests
- Ensure that all validations are performed as per standard

Authentication Token Standard NYS-S14-006

What it is

- Identifies appropriate two-factor authentication (2FA) authentication tokens for users at each Identity Assurance Level.

Relevance to DSRIP

- Identifies allowable 2FA token types to enable remote access to DOH Medicaid data

How it works

- Defines requirements for meeting AL3 using various token types
- Defines password policies for AL3
- Defines allowable 2FA token types
- Outlines related NIST FIPS 140 requirements for tokens

What you need to do

- Use the standard to identify appropriate authentication tokens to authenticate users, according to their Identity Assurance Level.

Relevant Policies and Standards

New York State http://www.its.ny.gov/tables/technologypolicyindex

- NYS-P03-002 NYS Information Security Policy
- NYS-P10-006 NYS Identity Assurance Policy
- NYS-S13-004 Identity Assurance Standard
- NYS-S14-006 Authentication Tokens Standard
- NYS-S14-007 Encryption Standard
- Section 367b(4) of the NYS Social Services Law
- NYS Social Services Law Section 369 (4)
- Article 27-F of the New York Public Health Law & 18 NYCRR 360-8.1

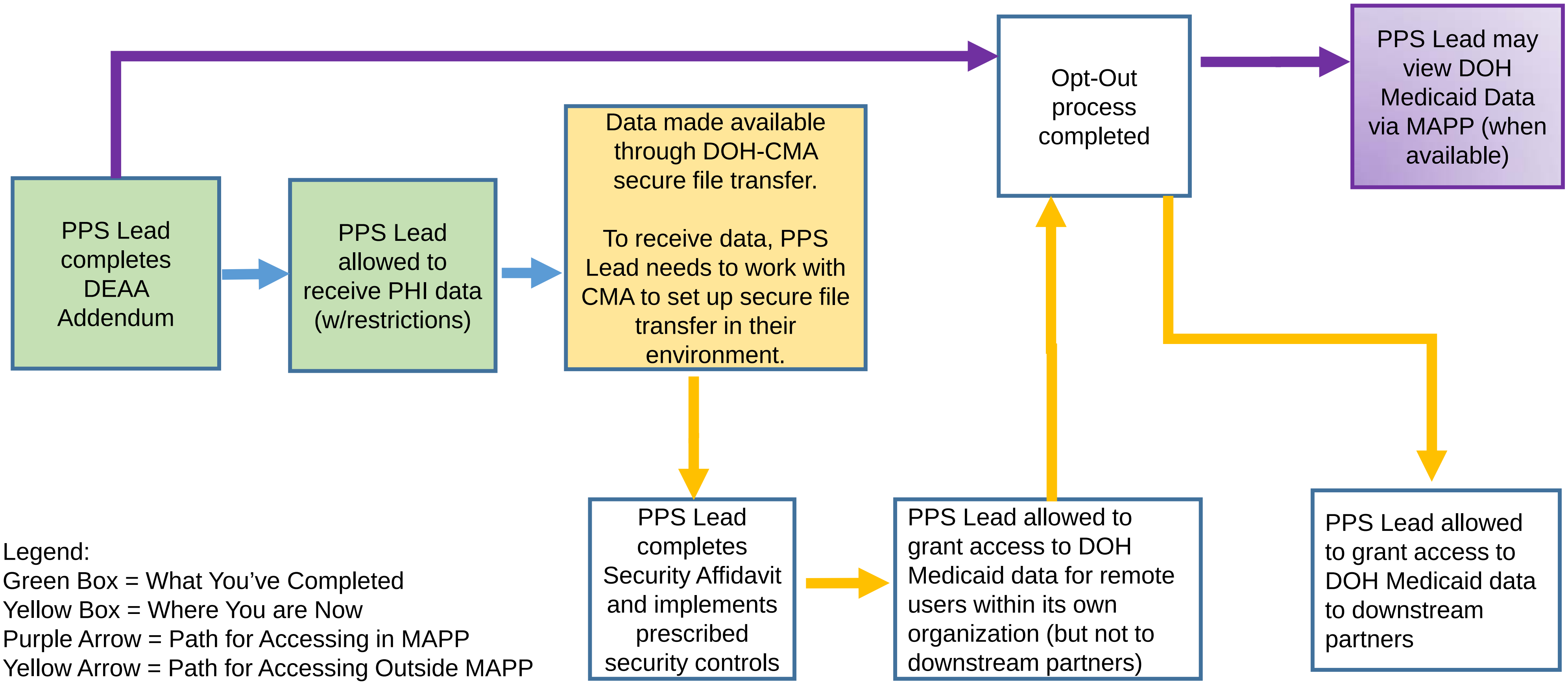
Federal

- NIST 800-63-2
- [ID] Management.Gov
- Social Security Act,42 USC 1396a (a)(7)
- Federal regulations at 42 CFR 431.302, 42 C.F.R. Part 2
- The Health Insurance Portability and Accountability act (HIPAA), at 45 CFR Parts 160 and 164

Processes and Controls for Accessing and Sharing DOH Medicaid Data

Rob Zeglen & Vince Hannon- NYSTEC

Process Flow for Release of DOH Medicaid Data



PPS Lead completes DEAA Addendum

PPS Lead allowed to receive PHI data (w/restrictions)

Data made available through DOH-CMA secure file transfer.

To receive data, PPS Lead needs to work with CMA to set up secure file transfer in their environment.

Opt-Out process completed

PPS Lead may view DOH Medicaid Data via MAPP (when available)

PPS Lead completes Security Affidavit and implements prescribed security controls

PPS Lead allowed to grant access to DOH Medicaid data for remote users within its own organization (but not to downstream partners)

PPS Lead allowed to grant access to DOH Medicaid data to downstream partners

Legend:
Green Box = What You've Completed
Yellow Box = Where You are Now
Purple Arrow = Path for Accessing in MAPP
Yellow Arrow = Path for Accessing Outside MAPP

Controls for Accessing and Sharing Data

PPS Lead Tasks Necessary for Data Sharing

- Two users from each PPS Lead Entity (PPS Lead) will be identity-validated & attested to by the PPS’ Gatekeeper per NYS Standards. These two users will be able to retrieve DOH Medicaid data containing PHI on behalf of their PPS.
- Obtaining DOH Medicaid data will be facilitated using the DOH-CMA Secure File Transfer Process.
- DOH Medicaid data should be downloaded to a network server. Decryption of data must be performed on a secure server.
- *Complete the Security Affidavit to enable expanded/remote access to DOH Medicaid data within the PPS. After the Opt-Out process is completed the data can be viewed by downstream providers.*

Choosing a Lead Data Partner for New Corporations (NewCo’s)

- NewCo’s have additional data sharing decisions to make with their co-lead partners.

Choosing a Lead Data Partner for NewCo's

- For data sharing purposes, DOH considers NewCo's (New Corporations) as those entities approved by CMS. These NewCo's may be comprised of several facilities serving as co-lead partners.

- NewCo's consisting of multiple co-lead PPS partners should choose one of the co-lead partners to retrieve and store the DOH Medicaid data in a secure system at the chosen co-lead's facility.

- The Gatekeeper who does the verification of the two tech-savvy users who will be able to retrieve DOH Medicaid data on behalf of the PPS entity should also come from the chosen co-lead organization.

- Other co-lead partners will be allowed to physically visit the chosen partner's facility and view DOH Medicaid data (provided they are named on the appropriate DEAA).

    - If other co-leads wish to store DOH Medicaid Data in their facilities, they must complete the security assessment process.

- Further guidance from the state will be made available shortly.

Secure File Transfer Process

How it works

- This is not part of MAPP but is a separate secure file transfer service.
- Requires selecting two IT-Savvy users, validating identity per NYS Standards, and working with DOH and CMA to configure those users' workstations, to receive the data securely.
- The process works over the internet and files are encrypted at rest and in transit, to ensure privacy of the data.

Note to PPS Leads

- DOH Medicaid data retrieved through secure file transfer prior to opt-out completion must be destroyed and an affidavit of data destruction sent to DOH.
    - PPS will not be able to retrieve new DOH Medicaid data (post-Opt-Out), until data destruction affidavit is received by DOH.

What's New in MAPP

Two-Factor Authentication (2FA)

- 2FA will be implemented by August 2015.
- The initial 2FA implementation will require users to have a NYS DMV-issued identification.
- When 2FA is implemented, all MAPP users will be asked to register a phone number that will facilitate 2FA for successive logins.
- Once 2FA is set up, a user logging into MAPP will need to do the following:
  - Users that opted to receive a text message to a **smartphone** will receive a text message containing a numeric security code. The code will be entered into the login screen to access MAPP.
  - Users that opted to use a **landline phone** will be presented with a numeric security code on the screen, and that code will be entered into the landline telephone, using the numeric keypad.
- DOH is working toward a path to access non-PHI data in MAPP that will not require 2FA

Opt-Out Process & Long-Term Data Sharing

Carlos Cuevas & Lyn Hohmann, DOH

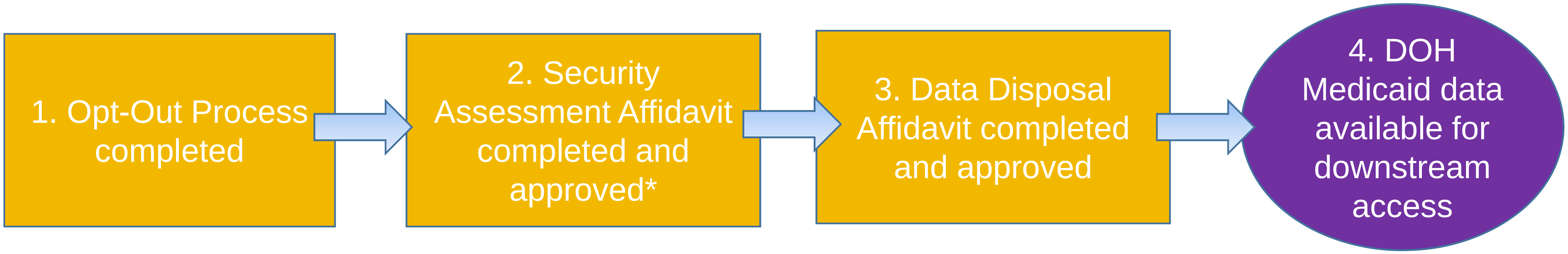
PHI: What You’re Getting

The following is the sequence of release of PHI Member/Claims lists:

- August– All Member Roster Released
- August– Initial Claims File with all attributed PPS members
- Fall – Member Claims Data available through MAPP
- Dec/Jan – Updated Member Rosters and Claims Data redacted to exclude members who have opted out or who have not been able to be contacted
- Future data releases will reflect the ongoing opt out process results

Long-Term Data Sharing Tasks

- Opt-Out process to be completed by DOH
- PPS Leads will be responsible for destroying Pre-Opt-Out DOH Medicaid data retrieved and submitting an affidavit (DEAA Attachment C) documenting the destruction has occurred.
    - DOH Medicaid data should not be mixed with PPS data, prior to completion of Opt-Out.
- For those organizations that completed the Security Assessment Affidavit^ and have received approval from DOH, once the Opt-Out process has been completed these organizations can share updated DOH Medicaid data with downstream partners.



1. Opt-Out Process completed

2. Security Assessment Affidavit completed and approved*

3. Data Disposal Affidavit completed and approved

4. DOH Medicaid data available for downstream access

*Make sure submission includes the most updated BAAs

^ PPS downstream partners will be able to view DOH Medicaid data containing PHI within MAPP without the PPS Lead undertaking the Security Assessment requirements.

About the DSRIP Opt-Out Process

- NYS is modeling the DSRIP consent process on the Medicare ACO model which is an opt-out model
    - Unless member formally opts-out of DSRIP data sharing, they are considered participating in data sharing.
- To "opt-out" means electing NOT to permit the sharing of any PHI and other Medicaid data held by the state with the PPS and its partners.
    - The member who "opts-out" will not have his/her Medicaid data shared with the PPS Lead Entity and partners.
    - DSRIP Performance measures will include opt-out members in the numerators and denominators, but drilldown to these members will not be available.
- A member can opt-out or opt-in for data sharing at any time.

About the DSRIP Opt-Out Process - Continued

- To begin the data sharing process, Medicaid is contacting all members by mail and providing each an opportunity to opt-out of the DSRIP data sharing with the PPS and partners.

- Until this first “opt-out” process cycle is complete, DOH-supplied PHI information cannot be shared with the PPS downstream partners.

- Medicaid will present the opt-out information to new members when they enroll. (This is an ongoing process.)

- **The DSRIP opt-out process only covers DOH Medicaid data that is shared with the PPS.**

  - The PPS may wish to review with its legal team the opportunity to notice itself as an “organized health care arrangement” per HIPAA and issue a PPS-specific “Notice of Privacy Practices” to address this data sharing.

DSRIP Opt-Out Letter

- Letter meets federal and state requirements related to PHI and privacy based upon review by NYS DOH, OMH, and OASAS

- DSRIP Project Advisory and Oversight Panel workgroup – the CBO/Cultural Competency workgroup reviewed/modified letter to ensure literacy issues minimized
  - This group consists of Medicaid advocates, beneficiaries, CBO representatives

- Contract being finalized with Opt-Out mailing vendor over the next 30 days

- Over 6 million letters going out this summer to Medicaid members

- Medicaid members have 30 days to respond

- A process has been built for finding alternative addresses for returned mail

- The initial Opt-Out process is scheduled for completion end of December 2015

Destruction of Data & Sharing Post Opt-Out

- Once the Opt-Out process is complete, in order to receive new DOH Medicaid data containing PHI, all previous iterations of DOH Medicaid data the PPS had received from the state must be destroyed.

- Per the DEAA, the PPS must submit an affidavit specifying the date and method(s) of destruction to verify the process.
  - Data Disposal Attestation Form – Attachment C of the DEAA

- PPS must keep a record of data use and certification records of destruction.

- Per NYS Sanitization Secure Disposal Standard (NYS-S13-003), acceptable methods of destruction include:
  - Shredding
  - Crushing
  - Forensic Cleansing
  - Degaussing

Questions and comments should be addressed to:

DSRIP email:
dsrip@health.ny.gov