NEW YORK STATE | Department of Health | Medicaid Redesign Team

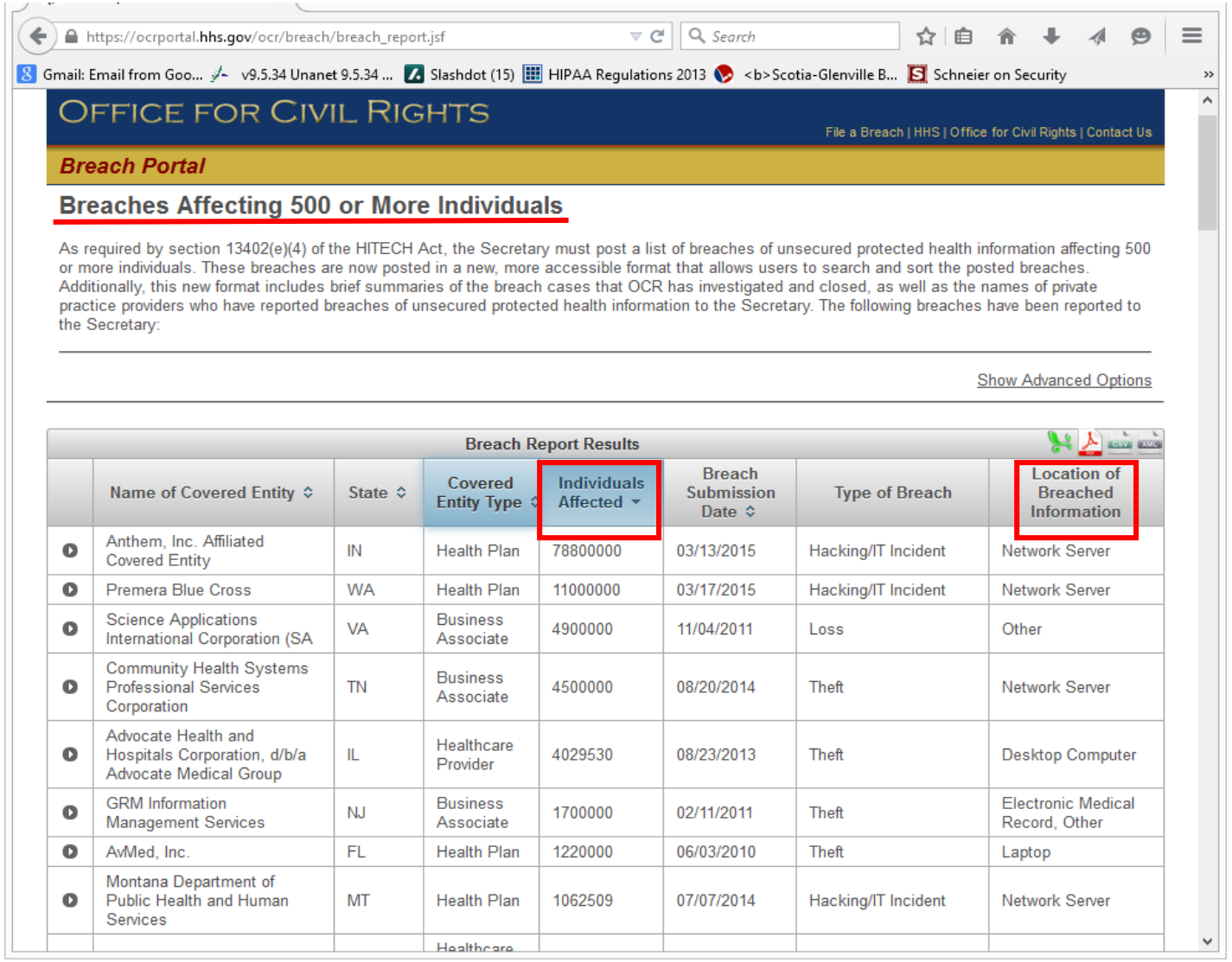
Protecting DOH Provided Medicaid Data

An overview of the recommended steps to secure access to DOH provided Medicaid PHI data and comply with updated DEAA requirements

Webinar Overview

- Purpose of DEAA Addendum?
- Steps Necessary to Support Data Security
- Identity Assurance Level Risk Assessment Example
- Medicaid Analytics Performance Portal (MAPP)
- Summary / Next Steps / Questions

Purpose of DEAA Addendum: Help Avoid Breaches and Public Shaming



https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

OFFICE FOR CIVIL RIGHTS

File a Breach | HHS | Office for Civil Rights | Contact Us

Breach Portal

Breaches Affecting 500 or More Individuals

As required by section 13402(e)(4) of the HITECH Act, the Secretary must post a list of breaches of unsecured protected health information affecting 500 or more individuals. These breaches are now posted in a new, more accessible format that allows users to search and sort the posted breaches. Additionally, this new format includes brief summaries of the breach cases that OCR has investigated and closed, as well as the names of private practice providers who have reported breaches of unsecured protected health information to the Secretary. The following breaches have been reported to the Secretary:

Show Advanced Options

Breach Report Results

Name of Covered Entity	State	Covered Entity Type	Individuals Affected	Breach Submission Date	Type of Breach	Location of Breached Information
Anthem, Inc. Affiliated Covered Entity	IN	Health Plan	78800000	03/13/2015	Hacking/IT Incident	Network Server
Premera Blue Cross	WA	Health Plan	11000000	03/17/2015	Hacking/IT Incident	Network Server
Science Applications International Corporation (SA	VA	Business Associate	4900000	11/04/2011	Loss	Other
Community Health Systems Professional Services Corporation	TN	Business Associate	4500000	08/20/2014	Theft	Network Server
Advocate Health and Hospitals Corporation, d/b/a Advocate Medical Group	IL	Healthcare Provider	4029530	08/23/2013	Theft	Desktop Computer
GRM Information Management Services	NJ	Business Associate	1700000	02/11/2011	Theft	Electronic Medical Record, Other
AvMed, Inc.	FL	Health Plan	1220000	06/03/2010	Theft	Laptop
Montana Department of Public Health and Human Services	MT	Health Plan	1062509	07/07/2014	Hacking/IT Incident	Network Server

NEW YORK STATE OF OPPORTUNITY. Department of Health

Purpose of DEAA Addendum: Help Avoid 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

What is the DEAA Addendum Requiring?

- Updated requirements for **access** to and **sharing** of DOH provided Medicaid Data

- Execution of an Identity Assurance Level (IAL) Risk assessment
  - *How much confidence do I need in the identity of the person accessing DOH Medicaid Data?*

- Implementation of necessary security controls based on IAL assessment to mitigate the risk of a PHI breach

- Alignment with NYS Policies and Standards

Relevant Policies and Standards

New York State

- **NYS-P03-002 NYS Information Security Policy**
- **NYS-S13-004 NYS Identity Assurance Policy**
- **NYS-P10-006 Identity Assurance Standard**
- **NYS-S14-006 Authentication Tokens Standard**
  http://www.its.ny.gov/tables/technologypolicyindex

Federal

- **NIST 800-63-2**
  http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf
- **[ID] Management.Gov**
  http://www.idmanagement.gov/

Webinar Overview

- Purpose of DEAA Addendum?
- **Steps Necessary to Support Data Security**
- Identity Assurance Level Risk Assessment Example
- Medicaid Analytics Performance Portal (MAPP)
- Summary / Next Steps / Questions

Overview of DEAA Addendum Steps

Step 1: PPS Lead Completes DEAA Addendum

- DOH reviews
- DOH Medicaid Data may shared with PPS Leads as per the following restrictions.

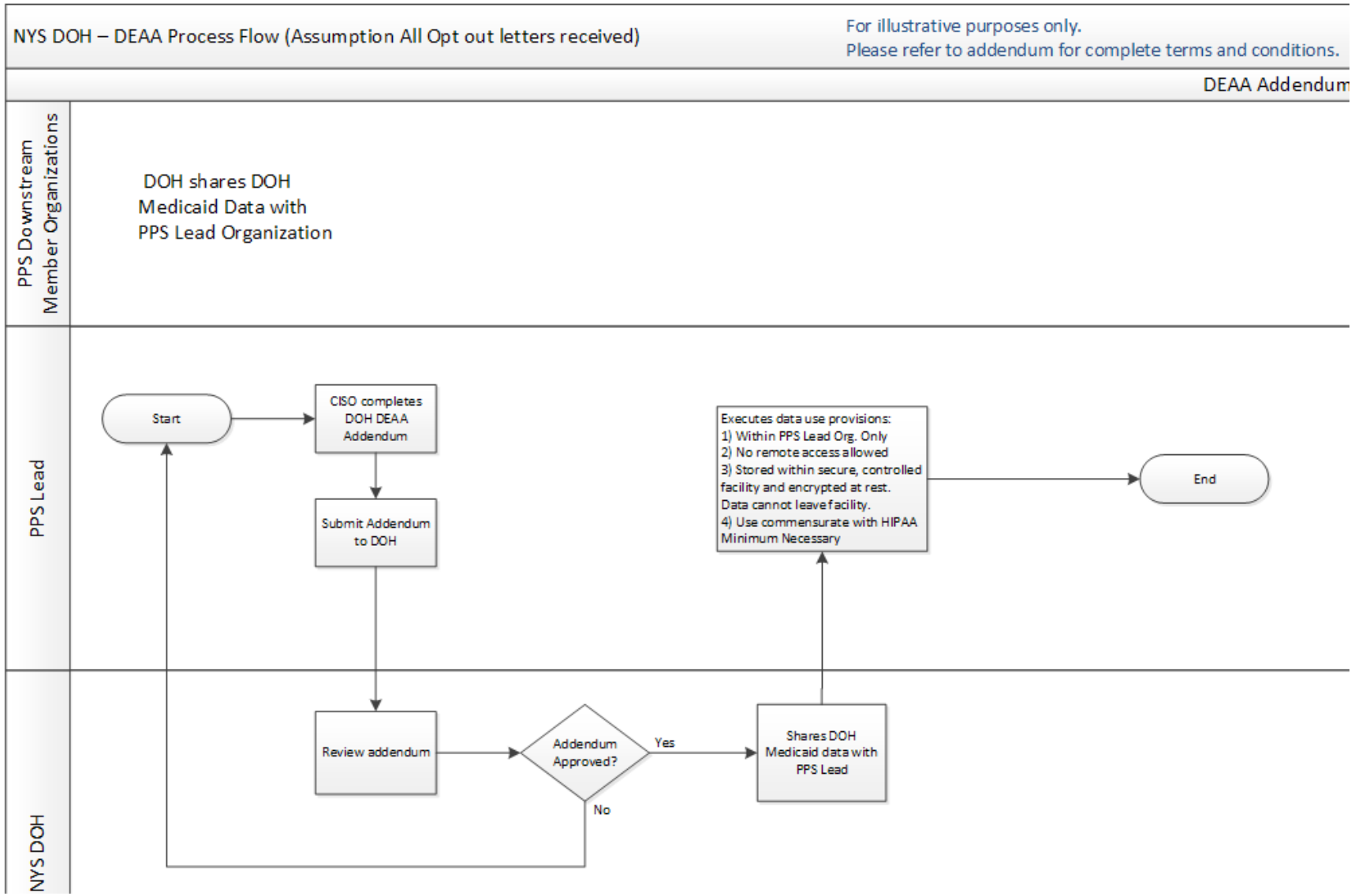
Table Below Outlines what a PPS Lead is permitted to do with
DOH provided Medicaid Data once DEAA Addendum is Approved

Allowed	Not Allowed
Employees or Corporate Affiliates*	Downstream providers, PPS Partners and Contractors
Local network access**	Remote access
Stored in single secure facility with controlled access	Stored in multiple locations, on removable media, uncontrolled access
Encrypted at rest as per HIPAA Security Rule	Unencrypted at rest
DOH Medicaid Data stays within facility	DOH Medicaid Data leaves facility

* Corporate Affiliates: There are certain PPS that have co-lead partners who may not be the same entity, but who have joined in close affiliation for the purpose of DSRIP. To view an entity as a corporate-affiliate (in order to share DSRIP PHI data before the assessment is complete), PPS co-leadership should be stated in the DEAA that acknowledges each party's responsibility to protect DOH Medicaid data.

** A local network is defined as a Local Area Network completely contained within a single building that has adequate physical security as per HIPAA guidance.

DEAA Addendum Workflow Diagram



NEW YORK STATE OF OPPORTUNITY. Department of Health

Overview of DEAA Addendum Steps

Step 2: Complete Identity Assurance Level (IAL) Assessment

- Determine *access points* that will enable **access** to DOH Medicaid Data
  - *Access points are typically IT systems where access is provided*

- Perform IAL Assessments for *each* access point and associated role
  - *Roles relate to levels of access provided to users (i.e.: summary access, full access), not to a professional role (i.e.: physician, nurse, administrator)*

- Implement necessary controls per IAL Assessment Results

What are the IAL Assessment Levels and Related Authentication Requirements

Identity Assurance Level	Authentication Required
AL1- Low or no confidence in the validity of the user's asserted identity	Single-factor (password)
AL2- Confidence in the validity of the user's asserted identity	Single-factor (password)
AL3- High confidence in the validity of the user's asserted identity	Multi-factor (multiple types)
AL4- Very high confidence in the validity of the user's asserted identity	Multi-factor (hardware token)

Overview of DEAA Addendum Steps

Step 3: Review contracts and update BAAs with downstream partners

- Ensure all downstream partners have signed BAAs with PPS Lead
- Verify that security controls are in place to allow access to DOH Medicaid Data*

Step 4: PPS Lead Completes Security Assessment Affidavit

- Security Assessment Affidavit provided by DOH (to be made available next week)
  - Attesting to DOH that required controls are in place
- Copies of BAAs and other relevant contracts submitted to DOH
  - Submit BAA for *each* downstream partner accessing DOH Medicaid Data*

* Once DOH approves the Security Assessment Affidavit, downstream partners may only access DOH Medicaid Data from the PPS Lead's approved access points

Overview of DEAA Addendum Steps

Step 5: DOH Review of Security Assessment Affidavit and materials received

- DOH may grant Applicant ability to allow access to DOH Medicaid Data
  - *Opt out process must be completed prior to PPS Lead allowing access to downstream partners*

Allowed	Not Allowed
Employees or Corporate Affiliates*, Downstream providers, PPS Partners and Contractors	Any downstream provider not covered in affidavit and submitted BAAs
Local network access**, Remote access	Access points not covered by Identity Assurance Level Assessment
Access to data stored on PPS Lead system in a read only and view only manner to downstream providers	Ability for downstream provider to download or modify DOH Medicaid Data
PPS member organization access to DOH Medicaid Data as per Security Assessment Affidavit	Other downstream partners not covered in Security Assessment Affidavit

* Corporate Affiliates: There are certain PPS that have co-lead partners who may not be the same entity, but who have joined in close affiliation for the purpose of DSRIP. To view an entity as a corporate-affiliate (in order to share DSRIP PHI data before the assessment is complete), PPS co-leadership should be stated in the DEAA that acknowledges each party's responsibility to protect DOH Medicaid data.

** A local network is defined as a Local Area Network completely contained within a single building that has adequate physical security as per HIPAA guidance.

Overview of DEAA Addendum Steps

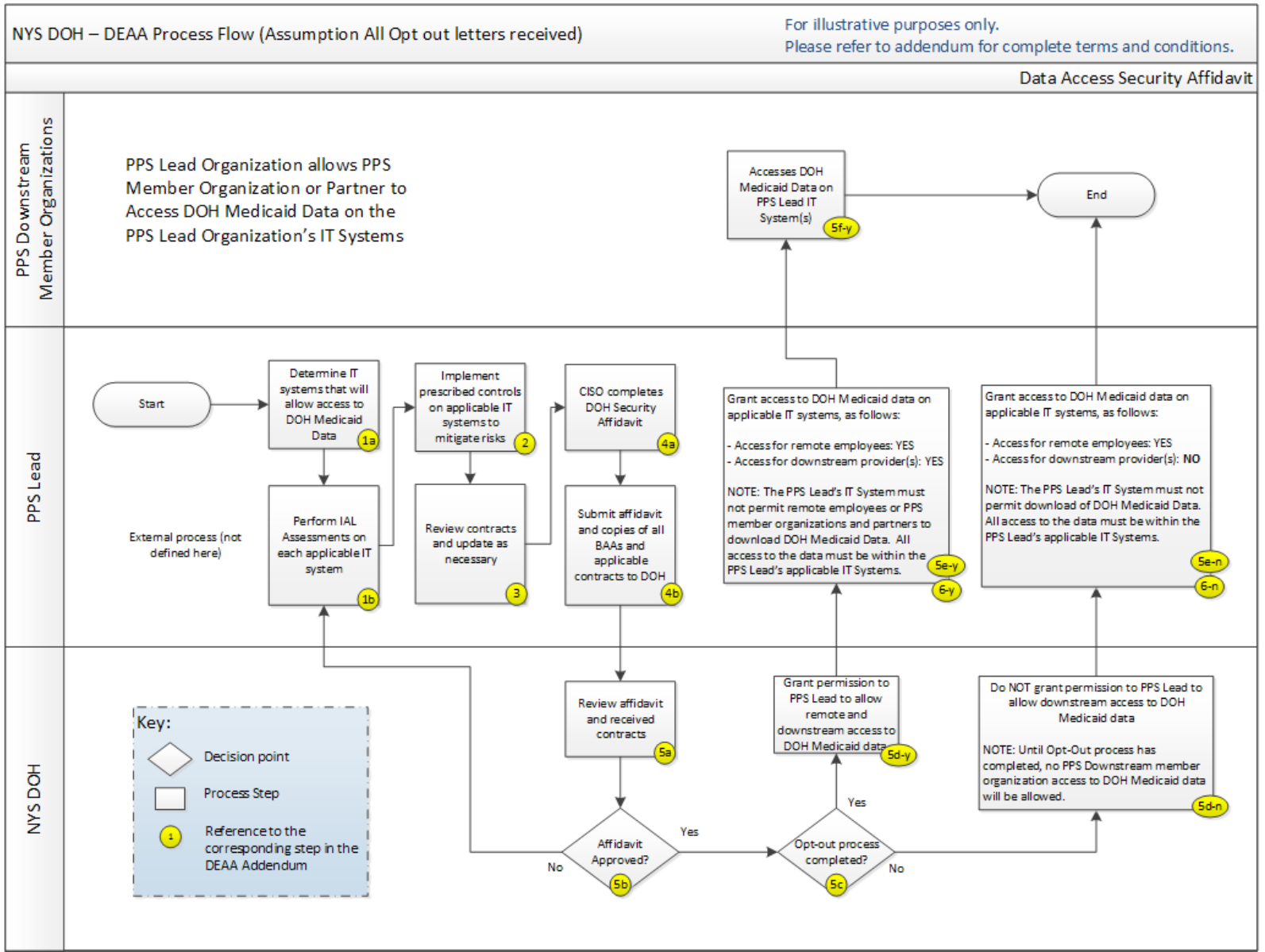
Step 6: Triggers for Identity Assurance re-assessments and re-submission of Security Assessment Affidavits by PPS Lead:

- Changes in business processes
- Realization of additional risk factors
- Annual re-assessment and re-submission of Security Assessment Affidavits

Step 7: DOH Compliance Assessments

- DOH reserves the right to perform compliance assessments for any Applicant, PPS partner organization or business associate

Overview of DEAA Addendum Steps



NEW YORK STATE OF OPPORTUNITY. Department of Health

Webinar Overview

- Purpose of DEAA Addendum?
- Steps Necessary to Support Data Security
- **Identity Assurance Level Risk Assessment Example**
- Medicaid Analytics Performance Portal (MAPP)
- Summary / Next Steps / Questions

What is a Risk Assessment?

Risk is a function of the ***likelihood*** of a given ***threat source*** exercising a particular potential ***vulnerability*** and the resulting ***impact*** of that adverse event on the organization.

A **Risk Assessment** is the process through which risk is identified, measured, and communicated to business stakeholders within an organization.

What is an Identity Assurance Level Assessment?

- Identity Assurance Level Assessment is different from a general/other risk assessments (HIPAA Risk Assessment)

- Identity Assurance Level Assessment is a narrowly focused assessment that covers
  - How we trust someone is who they claim to be
  - Potential impact to the security and integrity of system if a person is not who they claim to be
  - Determination of system's identity assurance level

Identity Assurance Level Assessment Steps

<u>Step 1</u>: Identify the Information Owner and Assemble the Assessment Team

- Identify the Information Owner and Chief Information Security Officer (CISO)
- Identify the Assessment Team Members
    - CISO
    - Data Owner
    - Business Analysts
    - Legal counsel
    - IT Staff

Identity Assurance Level Assessment Steps

<u>Step 2</u>: Collect System Information

- Information on data access points and how the DOH Medicaid Data is being accessed
  - (E.g., application, email, bulk file transfer, EHR system)

<u>Step 3</u>: Identity User Roles (as applicable) for each access point

- Assessments needed by role

Identity Assurance Level Assessment Steps

Step 4: Determine Identity Assurance Level for Each Role

Step 4a: Identify the Transactions a User Can Perform

- Inquire*
- Create
- Modify
- Delete

Step 4b: Determine and document the set of potential consequences associated with the transactions

* D*ownstream PPS partners may only possess this role*

Identity Assurance Level Assessment Steps

Step 4c: Assign impact levels based on consequences to the entity or authorized user

Step 4d: Use the impact levels to determine the identity assurance level for each role

- The system's identity assurance level will be based on the right-most checked impact level on the Identity Assurance Assessment.

Step 5: Identity Assurance Level Sign-off by the CISO

Assessment #2 Example

Webinar Overview

- Purpose of DEAA Addendum?
- Steps Necessary to Support Data Security
- Identity Assurance Level Risk Assessment Example
- **Medicaid Analytics Performance Portal (MAPP)**
- Summary / Next Steps / Questions

Medicaid Analytics Performance Portal (MAPP) High Level Overview

MAPP: Medicaid Analytics Performance Portal

- Multi-factor authentication to MAPP (Target Summer 2015)
- Supports Health Home Care Management needs
- Supports DSRIP Technology needs around:
  - DSRIP Provider Networks
  - DSRIP Attribution / Member Rosters
  - Quarterly Reporting
  - Performance Management utilizing Salient tool and;
  - Advanced Analytics using 3M/Treo Grouper capabilities

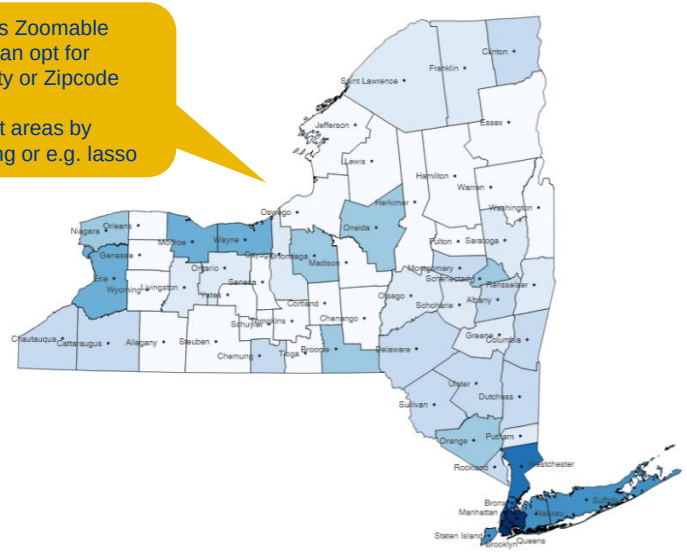
MAPP Performance Capabilities (Target Fall 2015)

- Integration with Medicaid Data Warehouse data
- DSRIP Performance measures calculations
- Drill down capabilities
  - PPS to Member Level
- Provide data that is actionable and timely

Indicator View – Drill-Down Capabilities

Key focus: 'what's underlying my score?'

- Map is Zoomable
- You can opt for County or Zipcode view
- Select areas by clicking or e.g. lasso



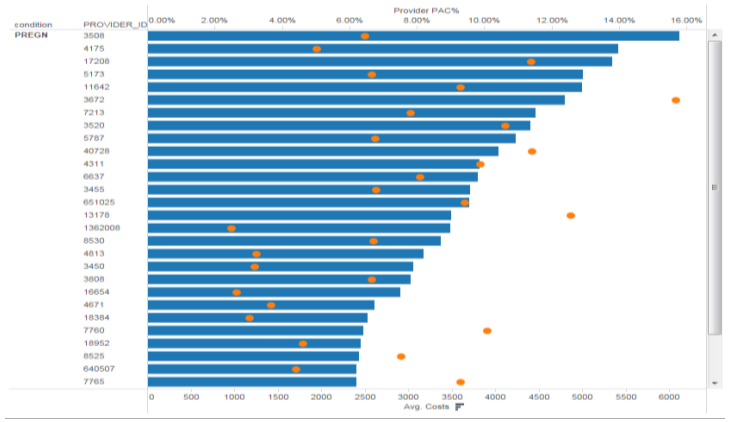
PQI Composite

- Top 10 lowest / highest performing PPSs/Hubs/MCOs/ counties/zipcodes

County ▼	Score ⬇	Trend YTD	Expected	Variance	$ Variance
Nassau	58%				
Suffolk	47%				
Westchester	45%				
Erie	43%				
Monroe	42%				
Onondaga	42%				
Rockland	40%				
Orange	39%				
Albany	39%				
Oneida	38%				
Dutchess	37%				

Greyed out in DY 1 – becomes operational in DY 2

Hospital



- Top 10 lowest / highest performing Hospitals / PCPs

Indicator
PQI Composite

Time Period
YTD

Year
2016

Population Filters
Greater Lake
Hub 2
MCO
County
Zip code
Age group
Gender
Ethnicity
Medicaid Status
Clinical Subpopulation
Providers

NEW YORK STATE | Department of Health | Medicaid Redesign Team

Webinar Overview

- Purpose of DEAA Addendum?
- Steps Necessary to Support Data Security
- Identity Assurance Level Risk Assessment Example
- Medicaid Analytics Performance Portal (MAPP)
- **Summary / Next Steps / Questions**

Summary

- MAPP is the preferred access method
- Even with DOH approval of the DEAA Addendum and Security Assessment Affidavit, sharing of DOH Medicaid Data is restricted
- DOH approval of a PPS Lead Security Assessment Affidavit will allow the PPS Lead to permit downstream partners to access DOH Medicaid Data through the PPS Lead's approved access points
  - *Even if PPS Lead has an approved Affidavit, no access permitted to downstream partners until Opt-Out process completed*
- Access to DOH Medicaid Data provided by a PPS Lead requires implementation of controls

Next Steps

- Sign and return DEAA Addendum (Due: COB, Wednesday, April 29th)
- Assess use of MAPP to eliminate need for Identity Assurance Level Assessment and implementation of security controls
  - For PPS Lead access and analysis
  - For downstream partners
- If necessary, complete Identity Assurance Level Assessment and implement security controls, and complete Security Assessment Affidavit
  - DOH will be making available the Security Assessment Affidavit template next week

Questions?

We'd like to hear from you!

DSRIP e-mail:

dsrip@health.ny.gov

'Like' the MRT on Facebook:

http://www.facebook.com/NewYorkMRT

Follow the MRT on Twitter: @NewYorkMRT

Subscribe to our listserv:

http://www.health.ny.gov/health_care/medicaid/redesign/listserv.htm

NEW YORK STATE OF OPPORTUNITY. Department of Health