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
### Purpose of DEAA Addendum: Help Avoid Breach Penalties

<table>
<thead>
<tr>
<th>Violation</th>
<th>Amount per violation</th>
<th>Max for violations of an identical provision in a calendar year</th>
</tr>
</thead>
<tbody>
<tr>
<td>Did Not Know</td>
<td>$100 - $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Reasonable Cause</td>
<td>$1,000 - $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Willful Neglect — Corrected</td>
<td>$10,000 - $50,000</td>
<td>$1,500,000</td>
</tr>
<tr>
<td>Willful Neglect — Not Corrected</td>
<td>$50,000</td>
<td>$1,500,000</td>
</tr>
</tbody>
</table>
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
  [Link](http://www.its.ny.gov/tables/technologypolicyindex)

Federal

• NIST 800-63-2
  [Link](http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf)
• [ID] Management.Gov
  [Link](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

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

* 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

NYS DOH – DEAA Process Flow (Assumption All Opt out letters received)

Start

DOB completes DOH DEAA Addendum

Submit Addendum to DOH

End

Review Addendum

Addendum approved?

Yes

Share DOH Medicaid data with PPS Lead

No

PPS Lead

PPS Downstream Member Organizations

DOB Shares DOH Medicaid Data with PPS Lead Organization

DEAA Addendum

For illustrative purposes only.
Please refer to addendum for complete terms and conditions.
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

<table>
<thead>
<tr>
<th>Identity Assurance Level</th>
<th>Authentication Required</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AL1</strong> - Low or no confidence in the validity of the user’s asserted identity</td>
<td>Single-factor (password)</td>
</tr>
<tr>
<td><strong>AL2</strong> - Confidence in the validity of the user’s asserted identity</td>
<td>Single-factor (password)</td>
</tr>
<tr>
<td><strong>AL3</strong> - High confidence in the validity of the user’s asserted identity</td>
<td>Multi-factor (multiple types)</td>
</tr>
<tr>
<td><strong>AL4</strong> - Very high confidence in the validity of the user’s asserted identity</td>
<td>Multi-factor (hardware token)</td>
</tr>
</tbody>
</table>
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**

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

* 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
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

**Step 1: 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

**Step 2: 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)

**Step 3: 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

* Downstream 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
# PQI Composite

## County Score

<table>
<thead>
<tr>
<th>County</th>
<th>Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nassau</td>
<td>58%</td>
</tr>
<tr>
<td>Suffolk</td>
<td>47%</td>
</tr>
<tr>
<td>Westchester</td>
<td>45%</td>
</tr>
<tr>
<td>Erie</td>
<td>43%</td>
</tr>
<tr>
<td>Monroe</td>
<td>42%</td>
</tr>
<tr>
<td>Onondaga</td>
<td>42%</td>
</tr>
<tr>
<td>Rockland</td>
<td>40%</td>
</tr>
<tr>
<td>Orange</td>
<td>39%</td>
</tr>
<tr>
<td>Albany</td>
<td>39%</td>
</tr>
<tr>
<td>Oneida</td>
<td>38%</td>
</tr>
<tr>
<td>Dutchess</td>
<td>37%</td>
</tr>
</tbody>
</table>

- **Top 10 lowest/highest performing** PPSs/Hubs/MCOs/counties/zipcodes
- Greyed out in DY 1 – becomes operational in DY 2

---

## 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

---

## Population Filters

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

---

## Time Period

- YTD
- Year
- 2016

---

## Key

- Focus: ‘what’s underlying my score?’

---

## Hospital

- Top 10 lowest/highest performing Hospitals/PCPs

---

## Map

- All widgets are linked – select one line/provider/county, all change

---

## Time Series

- Current Trend: 2014
- Previous Trend: 2013
- Historical Data: 2012

---

## 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