



## Department of Health

ANDREW M. CUOMO  
Governor

HOWARD A. ZUCKER, M.D., J.D.  
Acting Commissioner

SALLY DRESLIN, M.S., R.N.  
Executive Deputy Commissioner

The New York State Department of Health, Office of Health Insurance Programs, requires that all Performing Provider System (PPS) Lead entities (a.k.a. the “Applicant”) receiving Medicaid data containing Protected Health Information (PHI) originating from DOH (hereafter referred to as DOH Medicaid data) assess the need for two-factor authentication (a.k.a. dual authentication) when accessing DOH Medicaid data whether it be for employee use within the PPS Lead’s IT systems or when providing downstream entities (PPS member organizations and PPS Lead contractors) access to DOH Medicaid data through the PPS Lead’s IT System. This assessment requirement also applies to PPS downstream partners if they so desire to utilize DOH provided Medicaid data, shared through the PPS Lead entity, on their IT systems.

The DEAA Applicant (PPS) lead entity, shall designate a Chief Information Security Officer (CISO) (ex.: Chief Information Officer, Chief Technology Officer or equivalent), to sign this addendum.

Following receipt and approval of this DEAA addendum by DOH, the Applicant may, at the sole discretion of the Department, be provided with access to DOH Medicaid data. Following receipt and approval of the Security Assessment Affidavit (described below), the Applicant (PPS Lead Entity) may share DOH Medicaid data remotely within its network IT system and allow downstream partners to have access to DOH Medicaid data via the PPS Lead’s IT System. After this DEAA Addendum is signed, the PPS Lead entity must complete the following steps before executing the Security Assessment Affidavit:

1. PPS Lead agrees to complete an Identity Assurance Assessment, as per the NYS Identity Assurance Policy [NYS IT Policy No.: NYS-P10-006 (<https://www.its.ny.gov/document/identity-assurance-policy>)], for each DOH Medicaid data access point that will store or process and permit access to DOH Medicaid data. Until the Identity Assurance Assessment is completed *and* risks are mitigated via applied security controls, DOH-provided Medicaid data may only be made available to users “within the PPS Lead Organization.”
  - a. The phrase “within the PPS Lead Organization” will mean “employees or corporate affiliates! having access to the information only on the local network<sup>ii</sup>”.
  - b. No one (including PPS Lead Organization employees and corporate affiliates) may be provided remote access (outside the local network) to the PHI data, until DOH has given approval that the PPS Lead may do so (step #5).
  - c. Additionally, any DOH Medicaid data must be stored in a secure facility with controlled access and encrypted as per the HIPAA Security Rule while at rest and cannot leave the PPS Lead building in any fashion. This means that all analysis of the data must occur within the building.
  - d. Furthermore, data may only be made available within the PPS Lead Organization, commensurate with the HIPAA Minimum Necessary Requirement of the Privacy Rule (45 CFR 164.502[b], 164.514[d]) and using appropriate and relevant security controls as per the HIPAA Security Rule.
2. Once an Identity Assurance Assessment is completed by the Applicant, identified risks will be mitigated via the implementation of controls, commensurate with the existing DEAA and NYS Policies (<http://www.its.ny.gov/tables/technologypolicyindex>.) and the Identity Assurance Standard [NYS IT Policy No.: NYS-S13-004 (<https://www.its.ny.gov/document/identity-assurance-standard>)] for each DOH Medicaid data access point that will store or process, or share Medicaid ePHI.
3. The Applicant will review its contracts and, where necessary, update BAAs with downstream PPS member organizations and business associates, as well as take steps to gain assurance from these entities that



## Department of Health

**ANDREW M. CUOMO**  
Governor

**HOWARD A. ZUCKER, M.D., J.D.**  
Acting Commissioner

**SALLY DRESLIN, M.S., R.N.**  
Executive Deputy Commissioner

necessary controls are in place, commensurate with NYS Identity Assurance Policy, so that these downstream partners may be eligible to access DOH Medicaid data from the Lead PPS' IT System.

4. The Applicant may then submit a Security Assessment Affidavit (template to be provided by DOH) to the Department of Health, to certify that the Applicant has implemented the necessary controls (including two-factor authentication) as necessary on its systems and it has taken appropriate steps to ensure that controls have been implemented by PPS member organizations and business associates, when accessing DOH Medicaid data on the PPS Lead Entity's IT System. Copies of all pertinent contracts and Business Associate Agreements must also be submitted to the Department, for DOH review. *Please keep in mind that an alternative to the Security Assessment Affidavit process would be to allow PPS employees, member organizations and business associates to access the PPS' Medicaid data via the Medicaid Analytics Performance Portal (MAPP).*
5. Following receipt of the Security Assessment Affidavit and review of all materials received, the Department may grant the Applicant an entitlement to share DOH Medicaid Data that is housed within its IT System, remotely within its network, as well as with its PPS member organizations and business associates, as listed in the Security Assessment Affidavit. This effectively removes the restrictions cited in 1a through 1c above, for the PPS Lead Organization's IT System.
6. Following any meaningful changes in business processes, due to the realization of additional risk factors, or at minimum, annually, the Applicant must re-conduct the Identity Assurance Assessment for each DOH Medicaid data access point and submit the results to the Department via an updated affidavit. Reported results must be kept on file by the PPS Leads.
7. The Department reserves the right to perform compliance assessments of any Applicant, PPS partner organization, or business associate, who is accessing and or sharing DOH Medicaid data under an existing DEAA. Additionally, this includes the ability to review any downstream PPS partner, consultant or BAA agreements.



# Department of Health

ANDREW M. CUOMO  
Governor

HOWARD A. ZUCKER, M.D., J.D.  
Acting Commissioner

SALLY DRESLIN, M.S., R.N.  
Executive Deputy Commissioner

## Please return this document to:

Caryl Shakshober  
Caryl.shakshober@health.ny.gov  
DUE: close of business on Wednesday, April 29th, 2015

## Affidavit

I, \_\_\_\_\_, certify on behalf of \_\_\_\_\_  
insert name of Chief Information Security Officer (CISO) insert name of PPS

that the above provisions have been acknowledged, agreed to and will be met prior to any data sharing (of DOH provided data).

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date

<sup>i</sup> 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.

<sup>ii</sup> 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.