NEW YORK STATE OF OPPORTUNITY. | Department of Health

ANDREW M. CUOMO
Governor

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

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

Frequntly Asked Questions (FAQs) – Data Sharing and Security within DSRIP

THESE FAQS REFLECT THE COMMON THEMES SURROUNDING THE CURRENT STATE OF DATA SHARING AND DATA SECURITY REQUIREMENTS BETWEEN THE DSRIP PROGRAM OPERATED BY THE NEW YORK STATE DEPARTMENT OF HEALTH (NYSDOH) AND PERFORMING PROVIDER SYSTEMS (PPS). THIS DOCUMENT PROCEEDS THE INFORMATION RELAYED DURING THE DATA SECURITY AND INFORMATION SHARING WEBINAR HOSTED BY NYSDOH ON JULY 7, 2015.

New Corporations (NewCo) & Data Sharing

Q: Is a NewCo required to store data at one of the co-lead locations, or can the NewCo set up a secure server to store data compliant with all policies and laws?

A: The NewCo PPS is subject to the same restrictions as non-NewCo PPS. Before the Security Assessment Affidavit is completed and approved, the PHI data must be stored at rest at a co-lead location on a secure server. The data cannot be stored on a remotely hosted server. Follow the guidance in the DEAA Addendum and Security Assessment Affidavit.

Q: Can the Department offer guidance to those NewCos that may consist of multiple partners, which are considered equally contributing to the composition of the NewCo.

A: The Department is actively working on creating an Amendment to the DEAA to acknowledge the multiple founding entities of the NewCo and recognize them as co-lead partners. However, access to data will remain restricted prior to the completion of the Security Assessment Affidavit and opt-out process. More information on NewCos and data sharing will be released shortly, and in the interim NewCo PPSs should follow the same procedures that have been outlined in the DEAA and DEAA Addendum.

Opt-Out Process

Q: What is the opt-out process?

A: The opt-out process refers to the DSRIP consent process where unless the Medicaid 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 PHI and other Medicaid data held by the Department to the PPS and its partners. DSRIP Performance measures will include opt-out members in the numerators and denominators, but drill- down information to these members will not be available. Members can opt-in or out of data sharing at any time.

Q: What is the status of those Medicaid beneficiaries who do not respond to the opt-out?

A: Medicaid beneficiaries are considered opted-in to PPS data-sharing unless they call the Medicaid Call Center to opt-out or return the opt-out form.

Q: How will the PPSs be notified of Medicaid members who do not want their data shared? A: There will

be no official notice. Those members who have selected to opt-out of DSRIP data sharing will not be refreshed in subsequent releases of the Member Roster files.

Q: Can the Department share the letter with the PPSs to educate their beneficiaries?

A: Yes, the letter can be shared after it has been finalized. The Department is working towards finalizing the opt-out letter mailing out in August.

Claims Data

Q: If we are to get claims data for all attributed patients, does that mean the PPS Lead will know which patients are attributed to the PPS? How will new Medicaid members be reflected?

A: Member rosters and claims data received by a PPS will reflect that PPS' attributed lives. The PPS receives all Medicaid claims for members within their PPS. If a member is not eligible for Medicaid on the day the extract is run the members won't be included in that claims file.

Q: What patient information is included in the claims?

A: MAPP will provide both a Member roster and a claims extract file to the PPS. The Member roster will provide a list of members attributed to the PPS and for each member include the member's name, birthday, member's county code, member address, member contact number, member's Medicaid identification number and gender. The claims extract file will provide a list of claims for the attributed members and will include the following PHI info on the member: member's name, birthday, member's county code, member's Medicaid identification number and gender.

Q: How will this claims data affect the data in Salient? Will there be PHI in Salient data?

A: The Department intends to provide PHI through Salient Interactive Miner (SIM) and Salient Performance Dashboards to the PPS' for authorized users. Salient is working with the Department to determine the requirements necessary for PHI views in SIM and develop a timeline for access. SIM and Performance Dashboards will not expose member level data for members who have opted-out. PPS users will still have the ability to view performance measures at the PPS (summary) level that include members who have opted out. No drill down to opted out members will occur.

Medicaid Analytics Performance Portal (MAPP) & 2-Factor Authentication (2FA)

Q: Are there any other ID's that will be accepted in lieu of a NYS DMV issued identification?

A: Currently, other means of identification will not be accepted to access MAPP when a 2FA login is deployed. This is because 2FA is tied to the NYS DMV vetting database.
The Department is working to build both a PHI and a non-PHI view, however a timeline has not been released for this future development.

Q: Will the Department expand MAPP user slots per PPS?

A: Not at this time. The Department expanded the MAPP user slots available to each PPS in the recent past (June 4, 2015). If a PPS requires an update to understand their current MAPP users they may request this information via the DSRIP email address: dsrip@health.ny.gov

Q: Will MAPP permit exports of the list of patient data including PHI for leads and partners in the Fall after 2FA is added?

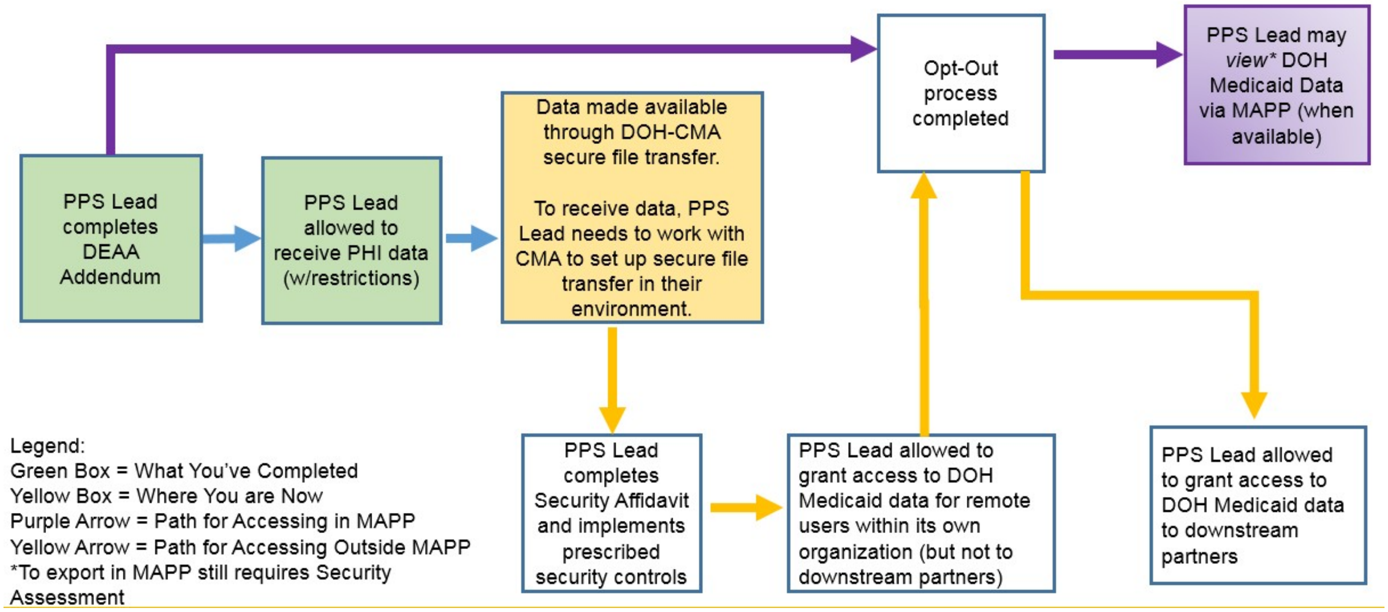
A: Yes, MAPP will have the capability to allow exports of PHI data from MAPP for ***authorized*** users and also allow view only access to patient data based on our Performance Module dashboards. Any MAPP user who requests export ability of PHI in MAPP will be considered a point of access within your PPS requiring execution of the Security Assessment procedure and Affidavit, and proceeds the opt-out process. PPSs granting view-only access to patient data within MAPP will not be required to complete a Security Assessment for those MAPP users approved for this access by their Gatekeepers.

Other Topics

Q: How does the definitions here apply to modern bulk or virtual storage pools such as NAS/SAN disk arrays? Is the use of commercial or certified secure deletion programs an allowable "Purge" option?

A: Should a NAS/SAN disk array be shared with other servers, the host server should implement an encrypting file system on its NAS/SAN volume, to protect the data at rest, wherever it may reside in the array. NYS standards at the following link address methods and tools to securely erase sensitive data, such as PHI: https://www.its.ny.gov/eiso/policies/security

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
*To export in MAPP still requires Security Assessment