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

Frequently 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). **BLACK** WRITING REFLECTS UPDATES AFTER THE JULY 2015 FAQS. **BLUE** WRITING REFLECTS WHAT WAS INCLUDED IN THE JULY 2015 FAQS PREVIOUSLY. THIS FAQ DOCUMENT UPDATED OCTOBER 15, 2015.

Data Sharing

Q: Can the Department provide examples of allowable secure transmission mechanisms that would allow PPSs to share PHI with downstream providers, including smaller providers?
A: PHI cannot be shared with any downstream providers until the Security Assessment Affidavit is completed, DEAA Attachment C finalized, and the opt-out process has completed. Any downstream providers receiving PHI from the PPS Lead Entity (PPS Lead) need to have Business Associate Agreements in place. The provider agreements may be specific to the PPS project selection.

Q: Assuming encrypted files could be transferred, would every recipient downstream provider need to meet the same "local server" requirements?
A: After the Security Assessment process is completed and the Affidavit approved by the Department, and following opt-out, your downstream providers may receive encrypted files with the same protections required of the Lead on their own local servers. Currently, before the Security Assessment, data destruction and opt-out process is finalized, no PPS Lead may transfer encrypted files to downstream partners. The PPS Lead and any downstream providers receiving data are expected to be compliant with the applicable NYS policies and standards, which are provided in the following link: https://www.its.ny.gov/eiso/policies/security.

Q: What does the Department mean by "remotely sharing PHI data with respect to the Lead Entity?"
A: Remote sharing refers to not being in the same physical location on the same physical network. The server used needs to be physically cabled to the workstation containing PHI data. This excludes the use of WiFi.

Q: Are PPS' outsourced I.T. systems or any other PPS vendor with whom significant PPS I.T. assesses reside considered "downstream partners" and cannot receive PHI?
A: Yes. According to the DEAA Addendum they are considered downstream partners.

~~**Q: CMS through the MSSP program allows dissemination of data to partners such as vendors who are remotely hosted (cloud service) if they are certified with a Data Use Agreement, are there options such as this offered in terms of data sharing within DSRIP?**~~
~~A: Until the Security Assessment, data destruction and opt-out process have completed, no remotely hosted vendors are permitted to access the data, including cloud providers. After opt-out has~~

~~completed, the Security Assessment Affidavit will still need to be completed on those partners using a cloud service.~~

Q: Should the PPS Lead in choosing a data storage center consider designating a secure server for the process of receiving PHI?
Yes, a secure server is necessary to store PHI data. The server must be located in a secure data center, on a secure network and access to the server must be protected with least-privileged access controls. The server should also encrypt data at rest.

Q: Can a RHIO named on the PPS DEAA download the files on behalf of a PPS?
A: They are still considered a subcontractor to the PPS Lead Entity, so the same data sharing restrictions apply as they would to any other PPS non-lead entity.

Q: Is the Affidavit acting as the Authority to Operate for the DOH?
A: Once the security assessment is received and approved by the DOH, then you have the authority to move forward with the controls you've indicated.

Q: Does a BAA suffice the requirements for subcontractors to access Medicaid claims data?
A: Yes, but the PPS, in turn, is attesting to DOH that the subcontractor has met all the necessary security requirements.

Q: Can a PPS' subcontractor be designated as the "gatekeeper role?"
A: Yes. Whether this makes sense, from a business perspective, depends on the level of autonomy that the PPS Lead wishes to permit for its subcontractors (BAs). The PPS Lead is still responsible for ensuring that the subcontractor applies the appropriate controls to protect the DOH Medicaid Data.

New Corporations (NewCo) & Data Sharing Processes

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.~~

A: The Department released on July 31st, 2015 an amendment to the DEAA for NewCos needing to recognize multiple co-lead partners as contributing to the administrative body of the PPS.

Q: We're in a NewCo and will be using the co-lead to house our data as we don't have any network infrastructure and leasing infrastructure. When we're filling out the SSP and we're including the network maps and other materials, are we including the information regarding where our server is going to be sitting on, we're not going to be giving remote access, they'll only be using it for server maintenance, etc.?
A: Include network and server information only for the environment that stores, processes, or transfers DOH Medicaid Data. Be sure to include networks and components that are used to access the data on the server, such as workstations, VMWare administration consoles, etc. If the environment that houses the data is not logically segregated from other network systems and components in your data center, it is important to include them, as well. Also include any pathways to networks that the applicable systems may have access, such as to the Internet.

Note:
If your organization is completing the DEAA NewCo amendment, one entity must be selected to house the data, at the current time. The SSP Workbooks describe the as-is state of controls of the system that houses the data, at the selected entity. Once both the NewCo DEAA amendment and the Security Assessment Affidavit are completed, it would then be permissible to share DOH Medicaid Data between NewCo systems, at additional Co-Lead locations.

Whenever the system storing, processing, or transferring DOH Medicaid Data changes or new systems are added, the SSP Workbooks need to be updated to reflect the changes.

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 by calling the Medicaid Call Center or submitting a signed opt out form.

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.~~
A: The letter is now on the DSRIP website in the Medicaid Member box. The mailing of the letter to Medicaid beneficiaries will occur in two phases. Phase 1 will begin mid-October 2015 and Phase II mailing to a larger group will occur mid-February to mid-March 2016. Thereafter mailings will occur on a monthly basis to newly enrolled Medicaid members.

Claims Data

Q: If PPSs 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.
A: Members who have formally opted out will also not be in the member roster or claims extract for that month's generated report.

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.

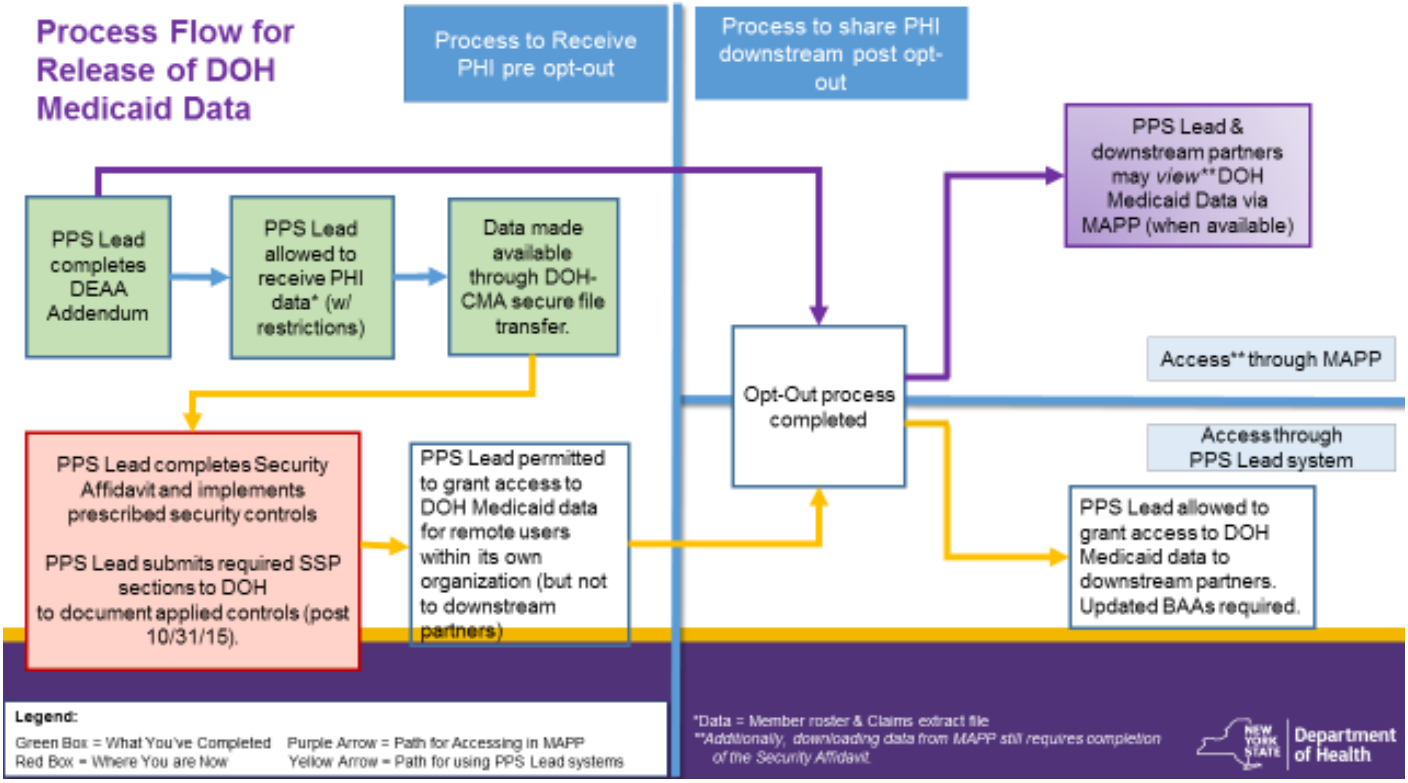
Medicaid Analytics Performance Portal (MAPP) & 2-Factor Authentication (2FA)

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
A: HCS coordinators have received instructions as to how to validate HCS users and register them for a 2FA login in instances where the user does not have a NYS identification.

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 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.

A: The new timeline for PHI data within MAPP is early 2016 for PPS Lead users, and after opt-out completes for PPS downstream partners.



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.

Q: If using a SAN not a NAS, which is a different storage fabric with different implications for the notation of encryption, how would the DOH requirements for pre-opt-out data differ between these technologies?
A: The DEAA Addendum requires pre-opt-out DOH Medicaid Data to be housed on an isolated system. This requirement can be implemented using SAN and NAS storage technologies, provided that the host server for DOH Medicaid Data performs FIPS 140-2 encryption on the logical volume that is created on the NAS/SAN being used for exclusively for DOH Medicaid Data, such that the keys for the encryption are unique to the host server and not accessible by any other host or the NAS/SAN hardware itself.

Q: Should we be planning for ALL 18 NIST SP800-53 R4 domains in future DSRIP phases? If yes - should we be planning for the long-term IT infrastructure now as opposed to a crawl and change approach over a multi-year time frame?
A: This will be investigated further and tabled for our next Data Security workgroup discussion.

Q: Can we "co-mingle" IP traffic on the same Internet link and VLAN that supports the encrypted VLAN traffic to the downstream FFTP server?
A: Yes, so long as DOH Medicaid Data is transferred in a strong-encrypted form.

Q: Can you please define what the difference is between "network access" and "local access?"
A: Local access is where a user or administrator logs onto the server through an interactive terminal connected directly to the server for that purpose. For virtual systems, this may be via a network, but the access is to the system terminal and results in a local interactive session on the server itself for that user. Network access is typically though a file share, web server, or similar method. This type of access doesn't result in an interactive shell or similar environment on the server itself.

Q: Regarding Dual Factor authentication, will subcontractor or vendors be require to abide by this requirement? If so, what is the proposed solution (username/password + token)?
A: Yes. An Identity Assurance Assessment will need to be conducted on the subcontractor/vendor systems, and the results of that assessment would identify the appropriate controls to be implemented. The acceptable solutions for authentication are provided in the NYS-S14-006 Authentication Tokens Standard.

Systems Security Plans

Q: If a PPS has several hubs that operate as an independent entity, is there any guidance as to how the SSP should be filled out? Should each hub fill out an SSP or can the SSP be submitted on the PPS level?

A: If the applicable information systems operate independently between hubs, it would warrant separate SSPs. All SSPs will require updates, and it would be easier to maintain updates for hubs that are operated independently, if separate SSPs were submitted.

Q: Our PPS deals with a number of vendors who work with the Medicaid data, will we be required to work with our vendors to understand what their controls are and document them in the SSP?

A: Yes, if the vendor is storing or processing DOH Medicaid Data, then controls for the applicable systems within the vendor environment would need to be documented in the SSP workbooks, and those systems would be expected to comply with DOH control requirements, as defined in the workbooks. PPS Leads should also ensure that they receive from each vendor working with DOH Medicaid Data a BAA that is countersigned by the lead PPS, including an assurance that appropriate security controls have been implemented, as advised.

Q: In terms of system use, if our DSRIP lead agency wants to analyze through analytical software (such as Microsoft Excel or Microsoft Access) but not transmit the DOH Medicaid data, does our SSP apply only to those systems with access to that database for analysis?
A: The SSP Workbooks apply to any system that will have access to the DOH Medicaid data, including those performing analytics. If a system will not store, process, or transmit DOH Medicaid Data, then the workbooks would not be applicable. It is important to note that once a system or platform starts to store, access, or transmit DOH Medicaid Data, the PPS will be responsible to add the system's controls to the SSP Workbooks.

Q: When we get the DOH Medicaid data, we will be putting it in an SFTP server. When we fill out the SSP, should we only address the SFTP server and anyone who accesses that?
A: That's correct, so long as that is the only system that will store, access, or process the DOH Medicaid Data, within the provisions of the DEAA Addendum. Should additional access be required, such as remote access or partner access, then the SSP Workbooks will need to include that information.

Q: We have engaged a third party and outsourced their services to receive the DOH Medicaid data. Does the vendor need to complete the SSP? Who is ultimately responsible for completing the SSP?
A: The PPS Lead Organization is ultimately responsible for ensuring SSP Workbooks are completed that account for all systems that store, process, or transfer DOH Medicaid Data, including third-party systems. Third-parties may participate in completing the workbooks, but ownership for ongoing updates is retained by the PPS Lead. Please note that for third-party systems, a business associate agreement would also be needed (signed by the PPS and the third party). The SSP workbooks provide excellent guidance that can be used, when going through the vendor selection process.

Q: What should we put in the narrative if we're not planning to fill out the SSP or will not use the data in the near term?
~~A: DOH is currently developing a template that will be distributed to PPS Leads within the next two weeks.~~
A: DOH has released a template PPSs should submit in the instance where the PPS has not taken data before the IPP Deadline of 10/31/15.

Q: Who is going to be reviewing the quarterly plans that PPS's are providing as submitting confidential data poses risk to organizations?

A: The DOH and the Independent Assessor will be reviewing all SSP workbooks that are submitted. The DOH reviews all responses to security requirements in confidence, and access will be restricted to only DOH and a small number of consultants that are subject to all BAAs on our behalf. KPMG will not be reviewing SSPs.

Q: For PPS' that are not receiving data at this time, when do we submit an Identity Assurance Assessment and documentation to engage a third party, are any outstanding SSPs due at that time?
A: It will be necessary to submit the currently-required set of SSP Workbooks and any previous workbooks, as per the submission schedule provided by DOH. For example, should your organization decide to receive DOH Medicaid Data in February 2016, the workbooks that were due on October 31 2015 and January 31 2016 would need to be submitted prior to receiving the data from DOH, and the schedule of due SSP Workbooks would continue with April 30 2016, as would be required for other PPS Leads that have been receiving DOH Medicaid Data.

Q: If our PPS is not receiving data by 9/30, are we expected to return our SSPs by the end of the quarter?
A: If you have expressed your intention to receive DOH Medicaid Data and have been involved in the process to be set up with Secure File Transfer from CMA, you will be expected to complete the required SSP Workbooks, by October 30, even if your organization has not yet completed the set-up and received the data from DOH.

Q: If you're hosting data on server with a 3rd party provider, it's going to be considered a multi-tenant server. What are the data security implications if you're renting a chunk of a server? How will this look in the workbook?
A: Renting a "chunk" of a server, rather than having the system logically isolated, is not permitted. The data needs to reside on a logically-independent server (such as a separate virtual machine instance) with its own dedicated, encrypted volume. E.g., volume encrypted by the operating system, such that only that operating system would have access to the volume. Hardware encryption in a NAS/SAN environment isn't acceptable, since the encryption is invisible to operating systems and applications and volumes are effectively unencrypted across these environments.

Q: In regards to submitting SSPs, is the PPS ultimately responsible for submitting the SSP (regardless of hub environment). If not, then provide an example when the PPS would not be responsible?
A: The PPS Lead organization is ultimately responsible for any DOH Medicaid Data access throughout the PPS and will be held responsible for completing the SSP Workbooks.

Q: If the PPS is responsible for the SSP and we have to put a point of contact, does the DOH only want one POC for the entire PPS or can it be multiple people?
A: It's up to the PPS's discretion. They can choose to designate one person as a "gatekeeper" for contact.

Q: How do the SSPs relate to the Data & Security Plan milestone?
A: The IPP narrative under the Data and Security Plan milestone does not currently address completion and submission of the SSP Workbooks. Including the completed workbooks as attachments will be our validation that your organization has completed the requirement for a data & security plan as iterated in milestone #5 within the IT section of the organizational application of the IPP.

Q: If the timing of the workbooks does not align with our stated timeline in the Implementation Report, which takes precedence?
A: The timeline originally submitted is the requirement. That said, it is unlikely that the SSP Workbooks would be submitted later than projected date in IPP. We'll be releasing additional guidance related to SSPs and IPPs.

Q: Do SSPs apply to data from Salient Interactive Miner stored locally and served within the organization?
A: Yes it does apply. Any system that applies to DOH Medicaid Data, no matter what the origin, applicable.

Q: Are we supposed to create data security plans on top of the SSPs?
A: The SSP Workbooks will form the control documentation for your security plan. Should your organization require, it is acceptable to include additional planning information with the SSP Workbooks, to form your security plan. Otherwise, DOH considers the workbooks to be your security plan.

Q: Does a SSP need to be completed for all PPS members or is it only MAPP data users and holders?
A: A set of SSP Workbooks needs to be completed at level of the system which stores or processes DOH Medicaid Data, and it must also include devices and networks that transfer that data. For example, if the data resides at the PPS Lead's data center, the SSP Workbook would be completed for the system(s) where the data resides in that data center, and it would include information on the networks, users, and endpoints through and from which the data will be accessed. Please refer to the Workbook instructions for definitions regarding Primary System versus Secondary System.

Q: If a PPS generates its own PHI data through various partnerships but not through the DOH. They will still need to protect the data based on standard protocols, but the DSRIP SSP does not apply there. Can you please confirm that this is the case?
A: SSP only applies to DOH-provided Medicaid data – although the DOH systems providing data do not have to be MAPP-specific. It applies to any system that will touch this data, as well. The SSP Workbooks do not have to be completed for systems or partners that will not be accessing DOH provided Medicaid Data. As a guide, the scope for completing the SSP workbooks should draw a "box" around just the systems, networks, and endpoints touching this DOH Medicaid Data. For example, if the PPS Lead receives DOH Medicaid Data and it is not shared and sits only within the PPS hospital, only the PPS hospital/staff would be covered in the SSP. If the PPS Lead generates its own PHI data (flowing up to the PPS from downstream and not top-down from the DOH), this data would not be included in the scope of the SSP (although it is expected that a similar level of controls would be enacted to protect that data, commensurate with HIPAA requirements).

Q: Are all controls listed in the SSPs required to be implemented? If they are not required, (for example, acceptable of PIV credentials) can the DOH please remove any controls that are not required of the PPS in order to reduce the size of workbooks and redundancy in writing "not applicable" and why it is not applicable?
A: It is necessary to consider the applicability for all of the listed controls, although not all controls would be applicable to a particular PPS Lead system configuration. For those that are found not to apply, it is important to include a brief reasoning for the decision. For example, if an organization does not utilize hardware-based authentication tokens, the controls listed in Workbook "IA - Identity and Authentication" that speak to hardware tokens might not be applicable. In such a case, explaining that

the organization has implemented an alternative authentication methodology and speaking briefly to that methodology would be sufficient, to complete these items.

Q: Regarding comment that organizations can satisfy the identification and authentication requirements in this control by complying with the requirements in Homeland Security Presidential Directive 12. Is this just a recommendation or a requirement?
A: Homeland Security Presidential Directive 12 defines high-level control objectives for authentication and identity validation, and it provides a timeline for compliance for Federal employees and contractors. These objectives are represented at the State-level through the NYS-P10-006 Identity Assurance Policy, NYS-S13-004 Identity Assurance Standard, and the NYS-S14-006 Authentication Tokens Standard. Compliance with these NYS documents will fulfill the directive for the Department of Health's purposes.

The SSP Workbooks are general-purpose documents that may list control requirements, which would not apply to a specific organization or have meaning in a particular business environment. Such is the case with "US Government PIV cards/DOD common access cards". In these cases, it is important to describe why the control(s) do not apply.

Q: Are the requirements for IA-2(1) the same as those listed for IA-2(3)?
A: They are not the same. The SSPs are very detailed in the delineation of controls, and there are requirements that seem very similar. In fact, in some cases, one applied control may satisfy several requirements. In that case, please reference the first requirement that describes the applied controls, for any other requirements that make use of that applied control, to satisfy those requirements. Please make sure that the referenced control has the documentation and artifacts that are needed to satisfy any items that reference that control. Using references can make it easy to forget to be as specific as is necessary or to provide applicable artifacts.

Q: IA-8(1) asks if we accept FICAM-approved third-party credentials. We are not a federal agency, so are we required to do this?
A: The SSP Workbooks are general-purpose documents that may list control requirements, which would not apply to a specific organization or have meaning in a particular business environment. Such may be the case with "FICAM-approved third-party credentials". In these cases, it is important to describe why the control(s) do not apply.

Q: Hardware token-based authentication – we do not use hardware tokens, but we do use software tokens. Therefore would page 24 not apply?
A: Correct. This is a great example for a control that would not apply and would need an explanation as to why it wouldn't. In this case, it would be sufficient to describe that the organization makes use of software tokens.

Q: Does the PPS Lead need to complete the SSP workbooks for only the DSRIP-related systems, for other systems that contain DOH Medicaid Data (beyond DSRIP), and for other non-Medicaid-related systems that contain PHI from other sources?
A: DSRIP-related systems: YES
Other systems that contain DOH Medicaid Data (beyond DSRIP): YES
Other non-Medicaid-related systems that contain PHI from other sources: NO (although recommended

as a best practice).

Q: If I use a cloud provider to store DOH Medicaid Data, would I still need to complete the SSP Workbooks?
A: Yes. The SSP Workbooks would need to be completed for the environment and system(s) being used to store DOH Medicaid Data on behalf of your organization. For a cloud service provider, the necessary information should be made available be the service provider, as part of their documentation, and that documentation may be referenced in the SSP workbooks. Include copies of all referenced documentation with your SSP Workbook submission to DOH.

Q: From the perspective of a small PPS, our resources are limited at this time to minimal IT staff, and it would be great to get feedback on what is expected and any guidance on how to effectively complete these workbooks by the deadline.
A: Although the workbooks seem like a big lift for many PPSs with small staffs, the Department is truly expanding efforts to protect PHI data as technologies and programs modernize, and creating a solid systems security plan is something the Department and CMS has been asking of all organizations that receive PHI. Also, as a note, two of the 4 workbooks that PPSs have received for the first set of workbooks - the IA and SC families - are a disproportionate lift to the remainder.