Data Sharing and Confidentiality

DSRIP Support Team

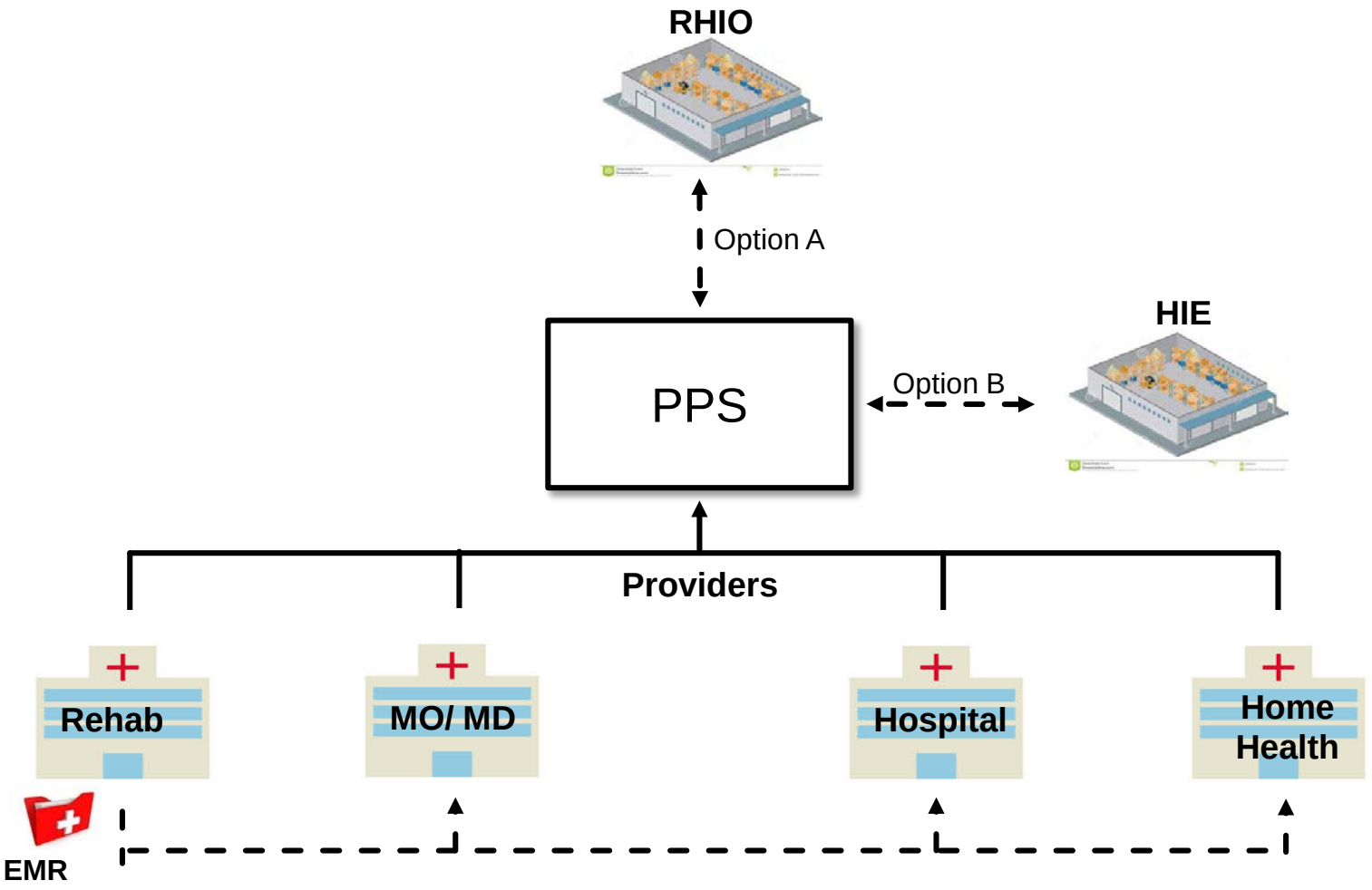
November, 2014

Contents

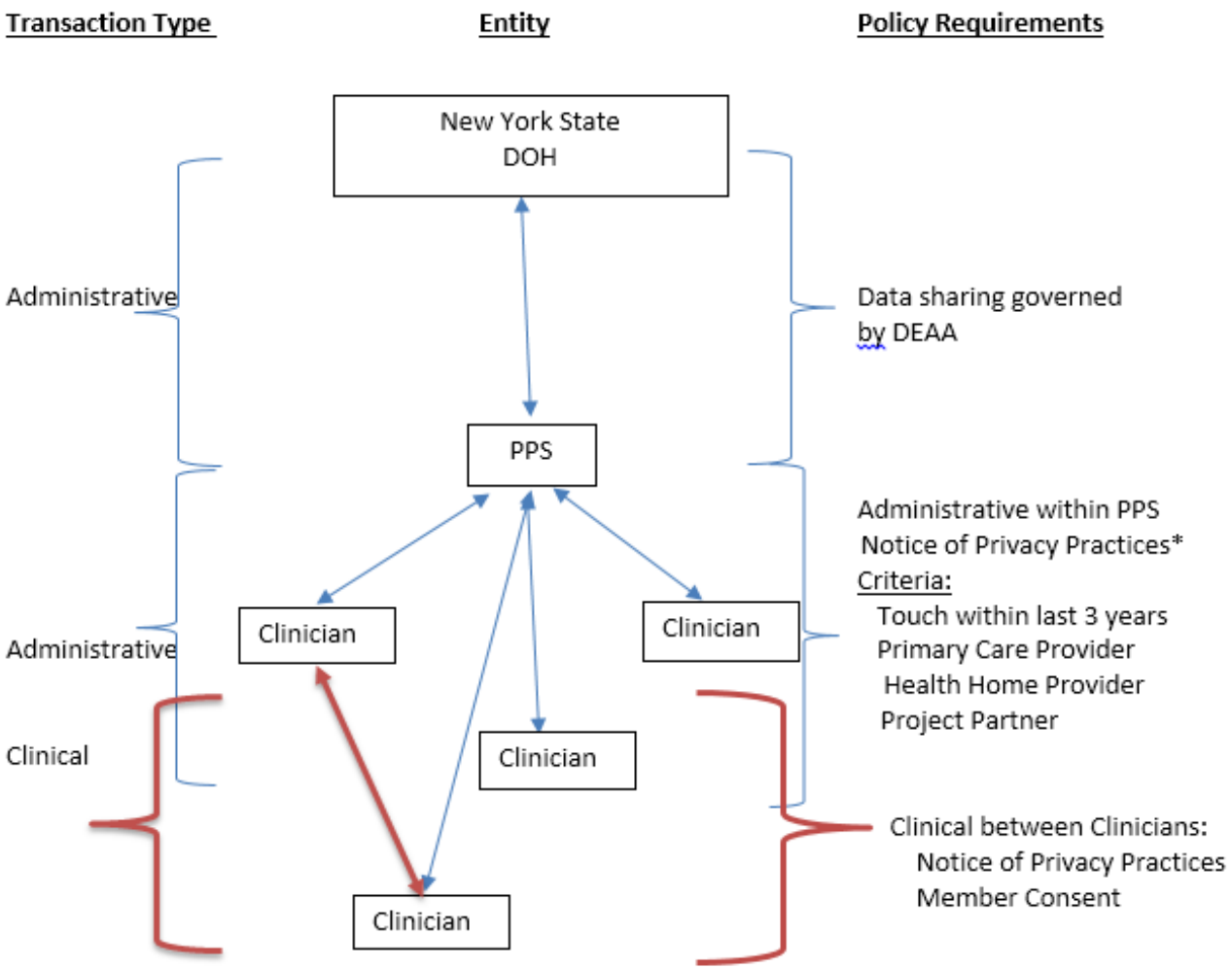
Introduction to Data Sharing and Confidentiality

PPS Partner Structure

PPSs will be exchanging data between multiple entities including HIEs and RHIOs, increasing the need to manage data security and confidentially to reduce possible data breach risk associated with data sharing



NYS DOH Proposed Data Sharing Model for DSRIP Utilizing "OPT OUT" Model in Place for ACOs



*Developed by PPS for its network partners

This model is built on the "OPT OUT" model supported by CMS for the Medicare ACOs.

In this proposed model, the PPS administration will need to notify the PPS Medicaid members of the PPS and its functions including need for data sharing. The Medicaid member then has the option to "opt out", in which case no data can be shared.

The opt out option only needs to be presented once for a PPS, but if a member in one PPS moves to another, the new PPS again has to give the member the option to opt out.

DSRIP Application Requires PPSs to Plan for Data Confidentiality and Sharing

1: Executive Summary

2. Governance

3: CNA

4: DSRIP Projects

5: PPS Workforce Strategy

6: Data-Sharing, Confidentiality & Rapid Cycle Evaluation 5%

7: PPS Cultural Competency/ Health Literacy

8: DSRIP Budget & Flow of Funds

9: Financial Sustainability Plan

10: Bonus Points

11: Attestation

PPS must include provisions for appropriate data sharing arrangements and a process for rapid cycle evaluation (RCE) supports requirements for reporting to the DOH and CMS

Data-Sharing & Confidentiality

- ❑ Plan for appropriate data sharing among partners
- ❑ Ability to share relevant patient information in real- time to ensure that patient needs are met and care is provided efficiently and effectively while maintaining patient privacy

Rapid-Cycle Evaluation

- ❑ Create an organizational unit within the PPS that is accountable for reporting results and making recommendations on actions requiring further investigation into PPS performance
- ❑ Plan for the use of collected patient data to:
  - evaluate performance of PPS partners and providers
  - conduct quality assessment and improvement activities
  - conduct population-based activities to improve the health of the targeted population.
- ❑ Mechanism to oversee the interpretation and application of results

What is Secure Data (or PHI)?

Information from a health care provider or a health plan can be PHI when it:

- Identifies an individual or could be used to identify an individual
- Describes the health care, condition, or payments of an individual or describes the demographics of an individual
- Information from a health care provider or health plan about an Individual's Physical or Mental condition, including:
  - Past history of a condition
  - Present condition
  - Plans or predictions about the future of a condition
- Information from a health care provider or health plan about an Individual's Health Care, including:
  - Who provided care
  - What type of care was given
  - Where care was given
  - When care was given
  - Why care was given
- Information from a health care provider or health plan about an Individual's Health Care Payments, including:
  - Who was paid
  - What services were covered by the payment
  - Where payment was made
  - When payment was made
  - How payment was made
  - Written information (reports, charts, x-rays, letters, messages, etc.,)
  - Oral communication (phone calls, meetings, informal conversations, etc.,)
  - E-mail, computerized and electronic information (computer records, faxes, voicemail, PDA entries, etc.,)

What Are PPS Considerations for Data Sharing and Confidentiality?

- **Does the PPS provide a document that spells out the responsibilities of the PPS and its partners?**
- **How does the PPS host assure that access to health data is limited to individuals who are authorized according to common privacy and security policies?**
- **How do organizations that contribute information to the PPS assure that they collect, store and communicate legally valid consumer consents for disclosure appropriately?**
- **How does the PPS host organization, data contributors, and data consumers transmit and store health information securely?**
- **What safeguards would ensure that only the minimum data necessary is accessed when the PPS use or access patient information for any reason beyond patient care?**
- **How do PPS hosts, data contributors, and data consumers use common interoperable security technology to assure confidentiality, integrity, authenticity, and accountability?**
- **How do PPS hosts protect and secure health information from possible theft or loss?**

What are Technical and Operational Vulnerabilities?

Common technical security vulnerabilities that affect most healthcare-related businesses:

- Lack of drive encryption for laptops and removable media
- Missing patches
- Weak operating system, application and database passwords
- Lack of content filtering and audit logging
- Insufficient malware controls for viruses, Trojans, spyware and rootkits

Common operational security issues include:

- A lack of responsibility and accountability
- Not knowing which sensitive healthcare records are stored/processed and where they're located on the network
- Weak or nonexistent security policies and plans
- Poor training and education for users
- System maintenance and monitoring deficiencies
- A lack of ongoing security and compliance assessments

Operational flaws come about, in large part, with:

- Poor leadership by executive management
- A lack of understanding of IT and security concepts
- A belief that all workers are trustworthy
- Increasing expectations for users to produce
- A shortage of IT and security expertise
- A lack of an established information privacy and security culture that fosters user buy-in

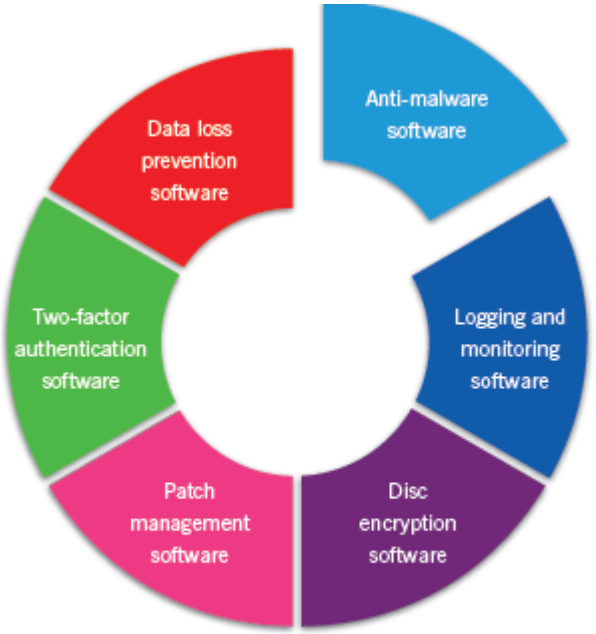


Figure 1: Practical security controls to minimize technical vulnerabilities

Leading Practices

Leading Practices: How Can You Reduce Your Risk?

HIMSS high level mitigation plan to preempt any security issues:

1. Identify key individuals who have authority and can take responsibility for managing this program.
2. Perform a high-level gap analysis to compare where you are now with where you need to be according to the specific regulations you're up against.
3. Perform an in-depth risk analysis to determine specific threats and vulnerabilities that need to be addressed, and document your findings.
4. Prioritize your specific needs.
5. Brief management on your findings.
6. Develop a budget.
7. Create the necessary policies, procedures and business processes to address your urgent and important findings.
8. Implement the proper technologies to help enforce your policies and carry out your procedures.
9. Train your users on what to do and what not to do

Leading Practices: How Can You Reduce Your Risk?

- **Form IT Governance Committee-** to review all relevant data sharing and confidentiality policies. Policies are reviewed and modified with partner organizations to ensure compliance and broad agreement. Policies are developed to address instances where data sharing protocols were compromised.
- **Conduct a survey of all PPS partners-** to understand who had electronic platforms (rather than paper-based processes) and the extent to which these systems are securely interoperable. Partners with paper-based systems were offered several options to move to an electronic platform:
    - PPS offers an EHR-light version to all partners
    - Each partner secures a compatible EHR platform independently
- **Promote use of real time data-** to ensure partners are accessing relevant patient data at the time of care. Built-in RHIO safeguards will provide another level of data security for efforts not to compromise patient trust.
- **Establish Data Sharing/Protection Protocols**
    - Participation Agreement - Designed to ensure that participants comply with the data sharing policies and procedures; explain the terms of the relationship, including roles, rights and responsibility of each party.
    - Business Associate Agreement (BAA) - is a person or entity that performs certain activities involving the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.
    - Data Use Agreement (DUA) - A covered entity may use or disclose a limited data set if that entity obtains a DUA from the potential recipient.

Considerations for Going Forward

Data Security Survey

YES	NO	
●	●	Employees sign confidentiality agreement
●	●	Confidentiality agreements with staff are signed on a routine basis at a _____ *(month)* interval.
●	●	The security practices of the organization have been audited with no material findings.
●	●	If material findings were noted, they have been corrected.
●	●	Written and explicit institutional policies and procedures are in place to deal with breaches of confidentiality.
●	●	Methods are proactive and in placed to monitor and detect the adherence to confidentiality protection procedures.
●	●	Data submissions are fully protected against legal discovery, including subpoena and freedom of information inquiries.
●	●	Organization or institutional penalties for misuse of confidential date and breach of confidentiality by staff exist, are available in writing , and are enforced.
●	●	Access to data files are restricted to specific project staff and access by non-project staff is not permitted.
●	●	An individual is formally designated to assure compliance with established institutional standards.
●	●	Specific sanctions for confidentiality violation can be imposed that include employee disciplinary action and any of the following: remedial training in confidentiality, loss of certification of competency, prohibition from future work with confidential data at the institution, discharge.

Data Security Survey Cont.

YES	NO	
●	●	Has developed and implemented education programs regarding confidentiality that includes information about the lack of security inherent in faxing, e-mailing, and other electronic data transfer, reminders about not using names or other personal identifiers in conversations in public areas such as open labs, elevators, or hallways; and reminders to employees of their special duty to maintain confidentiality when research involves individuals they know personally.
●	●	Formally credentials staff who have received confidentiality training.
●	●	Conducts a routine evaluation of skill and performance with regard to protection of confidentiality an identifies re-training needs based on performance.
●	●	Routine evaluation of employees' skill and performance is conducted.
●	●	Re-training needs are based on performance indicators, either for individuals groups.

Data Security Survey Cont.

YES	NO	
●	●	Authentication of users by means of passwords or digital ID.
●	●	Access control by means of role-based authentication/access, locked server room, and an internal firewall.
●	●	An audit trail that documents who, when and for what purpose data (including paper) was accessed.
●	●	A disaster prevention and recovery plan including adequate fire and entry alarms where data are stored; a fireproof file space for paper, routine backups of electronic data at intervals appropriate for the rate if data accrual; and offsite of backups (e.g., a safe deposit box).
●	●	External firewalls in places to prevent remote access by unauthorized users.
●	●	Virus checking is routine as are updates to the data files and engines to provide maximum protection of data files.
●	●	System assessment including diagnostics runs and external audits conducted regularly to insure the integrity of the system.
●	●	Data that are sent and received in conjunction with _____ *(Registry)* activities are electronically encrypted.
●	●	A data retention schedule is defined which includes a notation of the date when files are destroyed.
●	●	Data file owners are notified when their file is destroyed.
		The transfer of data is accompanied by:
●	●	A data-transfer agreement incorporating confidentiality standards to ensure data security at the recipient site and set standards for the data use at the recipient site.
●	●	A paste (electronic) or stamp (paper) on all records containing identifiable data as a reminder of the need for special handling.
●	●	Telecommuting and the use of home offices maintains the same level of security and procedures to address special issues, including data-transfer agreements, secure transmission procedures, and encryption. Additional safeguards are also followed, including: maintenance of minimal data on home computer, use of electronic screen savers, and password control at home.

Data Security Survey Cont.

YES	NO	
○	○	Restricting access to data-storage areas, the use of locked file rooms or cabinets in limited-access areas, a forms tracking log for any external disclosures, and a sign-out system for internal use of data.
○	○	Development and implementation of policies by institutions for the secure transport of information from one physical location to another.
○	○	Assuring confidentiality of written evidence that a patient is on a specific research study; for example, logs or lists of screened individuals or participants should not be left out on desks or in other open-access areas.
○	○	Safeguarding of ancillary records, e.g., pharmacy records, data on patients screened for clinical trial participation, etc.
○	○	Situating FAX machines in secure or limited-access areas; use of pre-coded phone number to eliminate dialing errors; cover sheets so data are not physically exposed; testing FAX machines to insure correct number and function; and de-programming FAX memory storage after use to prevent recovery of confidential information.
○	○	Employing established shredding procedures for disposal of documents after use.
○	○	Hardcopy information of sensitive information sent outside of the department is protected.

Disclaimers

This document was prepared by the Delivery System Redesign Incentive Payment (DSRIP) Support Team (DST). The advice, recommendations and information in the document included with this notice were prepared for the sole benefit of the New York State Department of Health, based on the specific facts and circumstances of the New York State Department of Health, and its use is limited to the scope of KPMG's engagement as DST for the New York State Department of Health. It has been provided to you for informational purposes only and you are not authorized by KPMG to rely upon it and any such reliance by you or anyone else shall be at your or their own risk. You acknowledge and agree that KPMG accepts no responsibility or liability in respect of the advice, recommendations or other information in such document to any person or organization other than the New York State Department of Health. You shall have no right to disclose the advice, recommendations or other information in such document to anyone else without including a copy of this notice and, unless disclosure is required by law or to fulfill a professional obligation required under applicable professional standards, obtaining a signed acknowledgement of this notice from the party to whom disclosure is made and you provide a copy thereof to New York State Department of Health**.** You acknowledge and agree that you will be responsible for any damages suffered by KPMG as a result of your failure to comply with the terms of this notice.

DSRIP Support Team