Adirondack Health Institute

Lead • Empower • Innovate

2018 DSRIP Compliance Training – AHI PPS

PRESENTED BY:

Alicia Sirk, MA, CHC, CHPC

Corporate Compliance and Privacy/Security Specialist

10/1/2018

What is DSRIP?

- Delivery System Reform Incentive Payment program = **DSRIP**
- DSRIP´s purpose is to fundamentally restructure the health care delivery system by reinvesting in the Medicaid program, with the primary goal of reducing avoidable hospital use by 25% over 5 years.
- DSRIP aims to restructure the health care delivery system through incentivizing and investing in provider collaborations, also known as performing provider systems (PPS).
- Up to $6.42 billion dollars are allocated to this program with payouts based upon achieving predefined results in system transformation, clinical management and population health, in accordance with certain terms and conditions imposed by the Centers for Medicare and Medicaid Services (CMS).
- Each PPS is required to commit to work on at least 5, but no more than 11 projects defined under the DSRIP program; each PPS must work with its Partners to identify which Partners will work on which projects.

Who are the Players?

- **PPS** – The entities that are responsible for creating and implementing a DSRIP project are called "Performing Provider Systems" or "PPS". Performing Provider Systems are providers that form a network based on contractual relationships and collaborate on a DSRIP Project Plan.
- **PPS Lead** – The PPS Lead is a safety net provider that serves as the convener of the performing provider system (PPS). The PPS Lead is responsible for
  - Overseeing the administration and operation of the PPS in accordance with the PPS governance structure
  - Serving as the recipient of funds from NYS
  - Distributing funds to the PPS partners in accordance with participation agreements and agreed-upon funds flow plans
- **PPS Partner** – The PPS Partner is a provider or other entity that has entered into a participation agreement with the PPS Lead to perform certain services and collaborate with a PPS in connection with the DSRIP program and/or one or more DSRIP projects.

Who are the Players? (cont.)

- **PPS Compliance Officer** – The PPS Compliance Officer is a PPS Lead employee who has been given responsibility for the day-to-day operation of the PPS's compliance program.
- **PPS Regional Compliance Workgroup** – A workgroup made up of Compliance Professionals from AHI (1) and partner organizations (16).
- **NYS Office of the Medicaid Inspector General (OMIG)** – The OMIG is the lead NYS agency responsible for improving and preserving the integrity of the NYS Medicaid program by conducting and coordinating fraud, waste, and abuse control activities for all State agencies responsible for services funded by Medicaid. The OMIG is empowered to conduct compliance reviews and audits of Medicaid providers, including PPS Partners and Leads.
- **DSRIP Independent Assessor** – The Independent Assessor is a DOH vendor responsible for ongoing monitoring of performance and reporting deliverables.
- **Contractors/Vendors** – Individuals or companies that are not PPS Partners but that are engaged by the PPS Lead, or by a PPS Partner, to perform services on their behalf in furtherance of the DSRIP program.

Who are the Players? (cont.)

- **Statewide Health Information Network of New York (SHIN-NY)** – A "network of networks" or "information superhighway" through which health information can be exchanged between and among providers regionally or throughout NYS, including for DSRIP purposes.
- **Regional Health Information Exchanges (RHIOs)** -- Organizations that facilitate health information exchange through the SHIN-NY among participating providers within a geographic region of NYS.
- **Qualified Entities** (QEs) – RHIOs that have been certified by NYS as meeting certain specified criteria.

DSRIP Overview

- All DSRIP funds will be based on performance linked to achievement of project milestones.
- In order for your practice/agency to receive these special funds, you are required to collaborate to implement innovative projects focusing on system transformation, clinical improvement and population health improvement.
- In order for your practice/agency to receive DSRIP funds and/or receive data, you are required to complete all AHI PPS Compliance requirements (including annual assessment questionnaires and training and attestations).

What is Corporate Compliance?

- Establishes a culture that promotes integrity and ethical behavior
- Provides assistance in complying with complex governmental regulations, including those related to fraud, false claims, theft or embezzlement, kickbacks or other violations
- Identifies issues of concern and detects and prevents patterns of improper conduct
- Safeguards public and private funds; helps control fraud, waste, and abuse

Why Do We Need A Compliance Program?

- It is important that we track the DSRIP dollars to ensure that the money is not connected with fraudulent behavior/practices.

DSRIP Corporate Compliance Program Applicability

- The DSRIP Corporate Compliance Program applies to all **Affected Individuals**:
  - Members of the Board of Trustees (**all**)
  - Executives (**all**)
  - Medical Staff (any involved in any aspect of DSRIP projects)
  - Employees (any involved in any aspect of DSRIP projects)
  - Volunteers (any involved in any aspect of DSRIP projects)
  - Students & Interns (any involved in any aspect of DSRIP projects)
  - Vendors (any involved in any aspect of DSRIP projects)
  - Agents (any involved in any aspect of DSRIP projects)
  - Independent Contractors (any involved in any aspect of DSRIP projects)

General NYS Compliance Requirements for Medicaid Providers, Including PPS Leads

- NYS Social Services Law §363-d,18 NYCRR Part 521 requires certain providers to annually certify, through the OMIG website that they have an "effective" compliance program.
- Required of providers that:
  - Are subject to Public Health Law A. 28 / 36 or Mental Hygiene Law A. 16 / A.31; *or*
  - Claim, order, bill, or receive more than $500,000 / 12 months from Medicaid
- NYS requires compliance programs to cover the following areas:
  - Billing and payments, e.g., claimed performance payments under DSRIP
  - Quality of care and medical necessity determinations
  - Governance
  - Mandatory reporting
  - Credentialing process; and
  - Other risk areas identified, e.g., privacy, conflicts, antitrust

Not all PPS Partners are required to have their own compliance programs under NYS law, but all must comply with the requirements of their PPS's compliance programs. Some PPS Partners that were not previously required to have compliance programs under NYS law may become required to do so, by virtue of receipt of DSRIP payments that result in their meeting the $500,000 threshold. All partners must receive Compliance training as per Master Partnership Agreements and assigned by AHI Compliance Dept.

Roles and responsibilities in DSRIP compliance

- **PPS Leads are required to design a compliance program for the PPS consistent with NYS requirements that focuses on the compliance risks and concerns within the DSRIP program, including:**
  - Policies and procedures that describe PPS compliance expectations
  - Disciplinary policies and procedures
  - Non-intimidation and non-retaliation policies
  - Process for reporting compliance issues to the PPS Compliance Officer
  - Process for risk identification, including auditing/monitoring PPS Partners' DSRIP performance
  - System for responding to compliance issues
  - Training and education of all affected employees and certain others

- **PPS Partners are required to:**
  - Participate in good faith in meeting the applicable metrics of the DSRIP program
  - Implement training and education provided by the PPS Lead
  - Develop or maintain a compliance program where required under NYS law
  - Observe contractual and other compliance requirements as required by the PPS Lead and state law, regulation, and policy
  - If you suspect that quality indicators are being falsely reported to satisfy DSRIP requirements, report it.
  - If you suspect that a provider is falsifying documentation on their Medicaid patient, report it.

***PPS Leads are not responsible for PPS Partners' non-DSRIP compliance programs or activities**.*

See Article II and Article VIII of AHI Master Participation Agreement.

PPS Compliance Policies and Procedures

- PPS Leads must have policies/procedures specifically relating to DSRIP issues [Element 1.]
- AHI PPS's compliance policies and procedures can be found at: http://www.ahihealth.org/ahipps/ahi-pps-policies-procedures/
- Policies can also be viewed and Attested to for your organization by your Compliance contact through the Navex Global platform.
- Any questions about the policies and procedures should be directed to AHI PPS Compliance Department.

Code of Conduct / Conflict of Interest Policy

➢ *Compliance is everyone's business; if you see something- say something*	➢ *Provide accurate and truthful information*
➢ *There is zero tolerance for retaliation for good-faith reporting*	➢ *Take an active role in compliance education*
➢ *Safeguard DSRIP funds and DSRIP Data*	➢ *Help to ensure medically necessary and quality care*
➢ *Ensure proper credentials and licensure*	➢ *No exclusion from government health care programs*
➢ *Conflicts of Interest* – Declare them, mitigate them, avoid them.	➢ *Protect patient confidentiality; other business information*
➢ If you are unsure about any of these, please ask us.	

Whistleblower Policy

- The Lead must have policy of non-intimidation and non-retaliation and support PPS Partners' compliance with this requirement [Element 8.]
- Roles and responsibilities:
  - PPS Leads are responsible for ensuring non-intimidation and non-retaliation with respect to their own staff.
  - PPS Partners must comply with this requirement with respect to their staff.
  - PPS Leads should support implementation of this element by their PPS Partners.
  - Each PPS must have a process for sanctioning or terminating participation in the PPS in the event of a PPS Partner's noncompliance with PPS policies, procedures or contractual requirements.

See Article VIII of AHI Master Participation Agreement.

Employee Whistleblower Protections (41 U.S.C. 4712)

Employers are prohibited from discharging, demoting, or otherwise discriminating against an employee as a reprisal for disclosing, to any of the entities listed at paragraph (B) of this subsection, information that the employee reasonably believes is evidence of gross mismanagement of a Federal contract, a gross waste of Federal funds, an abuse of authority relating to a Federal contract, a substantial and specific danger to public health or safety, or a violation of law, rule, or regulation related to a Federal contract (including the competition for or negotiation of a contract). A reprisal is prohibited even if it is undertaken at the request of an executive branch official, unless the request takes the form of a non-discretionary directive and is within the authority of the executive branch official making the request.

An employee who believes that he or she has been discharged, demoted, or otherwise discriminated against contrary to the policy in 3.908–3 of this section may submit a complaint with the Inspector General of the agency concerned. Procedures for submitting fraud, waste, abuse, and whistleblower complaints are generally accessible on agency Office of Inspector General Hotline or Whistleblower Internet sites.

See Article VIII of AHI Master Participation Agreement.

Report DSRIP Compliance Concerns

PPS Lead must have established process of reporting compliance issues to Compliance Officer, including by an anonymous/confidential method [Element 4]. ***If you suspect a breach of fraud, waste, or abuse of DSRIP funds, report it to the AHI Compliance Department:***

- **Anonymous Compliance Hotline**: 844-386-2242 (externally)
- **Chief Operating and Compliance Officer**:
  Jeff Hiscox ~ 518-480-0111 ext. 109 or
  email: **ahicomplianceteam@ahihealth.org** / jhiscox@ahihealth.org
- **Corporate Compliance and Privacy/Security Specialist**:
  Alicia Sirk ~ 518-480-0111 ext. 110 or
  email: **ahicomplianceteam@ahihealth.org** / asirk@ahihealth.org
- **AHI Online Form or Mail-In Paper Form (http://www.ahihealth.org/who-we-are/contact-us/ahi-corporate-compliance-report-form/)**

All reports are confidential and may be anonymous
*****It is illegal for anyone to retaliate against an employee who reports suspected fraud, waste, or abuse.*****

Online Compliance & Customer Service Reporting

AHI Corporate Compliance/Customer Service Reporting

Adirondack Health Institute Corporate Compliance Reporting

Our Corporate Compliance program's mission is to ensure that the service delivered to our stakeholders and the business conducted is done so honestly, ethically and in accordance with Federal and State law and regulations. Utilize this form for questions and concerns regarding Adirondack Health Institute's corporate compliance with Federal and State law and regulations or call the 24-hour Anonymous Hotline at **844.386.2242**.

Learn more and submit the AHI Corporate Compliance Reporting form or call the 24-hour Anonymous Hotline at **844.386.2242**.

Adirondack Health Institute Corporate Compliance Reporting (3rd Party – EthicsPoint)

Our Corporate Compliance Department wants to ensure you have multiple venues to report any compliance concerns you may have. We have set up a 3rd party reporting platform that will provide additional comfort for reporting concerns, both confidentially and anonymously. In order to utilize this method, please call **844.251.4252** to speak with a representative who will help you complete your report, **or** click on EthicsPoint to be redirected to the 3rd party site where you can complete your report electronically.

Adirondack Health Institute Customer Service Reporting

Our employees, board members, volunteers, interns, independent contractors and vendors work with the public to provide services and expertise. Please utilize this form for questions and concerns regarding AHI customer service and program delivery.

Learn more and submit the AHI Customer Service Reporting form.

http://www.ahihealth.org/ahi-corporate-compliance-report-form-2/

Report Compliance and Privacy Breaches Cont.

If you suspect a breach of privacy, confidentiality or fraud, waste, or abuse report it to the AHI Compliance Officer:

In situations where you prefer to place an anonymous report in confidence, you are encouraged to use this hotline, hosted by a third party hotline provider, EthicsPoint. You are encouraged to submit reports relating to violations stated in our Code of Conduct, as well as asking for guidance related to policies and procedures and providing positive suggestions and stories.

The information you provide will be sent to us by EthicsPoint on a totally confidential and anonymous basis if you should choose. You have our guarantee that your comments will be heard.

- **Confidential/Anonymous 3rd Party Reporting Line (EthicsPoint)**: 844-251-4252 (speak with a representative who will help you complete your report)

- **Confidential/Anonymous 3rd Party Compliance Reporting (EthicsPoint Online)**: https://secure.ethicspoint.com/domain/media/en/gui/54205/index.html

All reports are confidential and may be anonymous

*****It is illegal for anyone to retaliate against an employee who reports suspected fraud, waste, or abuse.*****

Compliance Reporting

Please report concerns about Fraud, Waste, Abuse, Safety, Privacy and Security

It is the Policy of AHIPPS to encourage prompt reporting, at the earliest reasonable opportunity, by employees, board members, clients, independent contractors and vendors of any activity or conduct in violation of any AHIPPS compliance policy or any federal, state or local laws or regulations pertaining to compliance related matters.

Examples include, but are not limited to:

- Medicare/Medicaid Fraud and Abuse
- Falsification of medical records
- Harassment or Discrimination
- Health, Safety, and Environmental Issues
- Questionable billing or coding activities
- HIPAA Privacy or Security Violations
- Any good faith concern
- Any form of retaliation against those reporting a potential violation in good faith

Call the Anonymous Hotline **844-386-2242** or the Anonymous 3rd Party Reporting Hotline **844-251-4252** (both available 24/7) or email the AHI Compliance Team at ahicomplianceteam@ahihealth.org or report online at www.ahihealth.org. Look for the AHI Corporate Compliance/Customer Service Reporting link.

All calls received on the hotline are confidential and messages may be left anonymously. Individuals leaving an anonymous message are encouraged to provide as many details as possible in order for AHI to conduct a proper investigation. Individuals reporting problems or concerns in good faith will be protected from retaliation, retribution or harassment.

Confidential vs Anonymous (Element 4)

Confidential vs. Anonymous:

- **Anonymous** means that you do NOT provide your name. If you choose anonymous reporting, be sure to provide enough details that we can investigate.

- **Confidential** means you provide your name, but request that we not disclose your identity as the reporter. We will do our best to shield your identity, but cannot guarantee that it will never be known (for example, we could be compelled to by an external agency investigation or a court order).

Reporting Fraud, Waste and Abuse of DSRIP Funds

- Workforce members who are aware of any violations of the code of conduct, false claims, or of any other inaccurate practices are expected to report their concerns to the AHI Compliance Department. Anyone who makes a good faith report to their immediate supervisor or the AHI Compliance Department, of a potential corporate compliance violation is specifically protected from retaliation.

- Reports can be made in person, by email [ahicomplianceteam@ahihealth.org], by online report form, by postal mail or phone call. Written reports may be made by completing a Corporate Compliance Report Form and mailing it to: AHI Compliance Department, 101 Ridge Street, Glens Falls, NY 12801.

- Compliance report forms may be completed anonymously and training on location of forms is provided to all AHI employees, executives, interns, volunteers, and governing body members, as well as all affected individuals of PPS Partners, during compliance training. Additionally, forms are available on AHI's website for contractors and agents of AHI, or other individuals as necessary.

Reporting Fraud, Waste and Abuse of DSRIP Funds (cont.)

- The confidentiality of the person making the report will be protected to the fullest extent possible. AHI prohibits retaliation or threats of reprisal against any person who reports a possible compliance violation. If retaliation occurs, it should be reported immediately to AHI's Compliance Department, CEO, or Board of Directors.

- AHI expects that all PPS Partners will comply with the compliance plan, including the requirements of monitoring, auditing, self-disclosure, and in reporting and assisting in the resolution of all compliance issues involving DSRIP funds. Any PPS Partner suspecting fraud, waste, or abuse of DSRIP funds is expected to report compliance issues at the earliest possible opportunity to AHI's Compliance Department via any method outlined in this plan. Failure to comply with any aspect of the compliance plan will result in disciplinary action up-to and including termination of contract with AHI, in accordance with general AHI disciplinary policies. Anyone who makes a good faith report to AHI's Compliance Department, of a potential corporate compliance violation is specifically protected from retaliation.

- In an effort to assure that all potential compliance issues are reported, AHI **requires** all PPS Partners to also have an anti-intimidation and anti-retaliation policy in place to protect any workforce member of its organization who makes a good faith report to AHI.

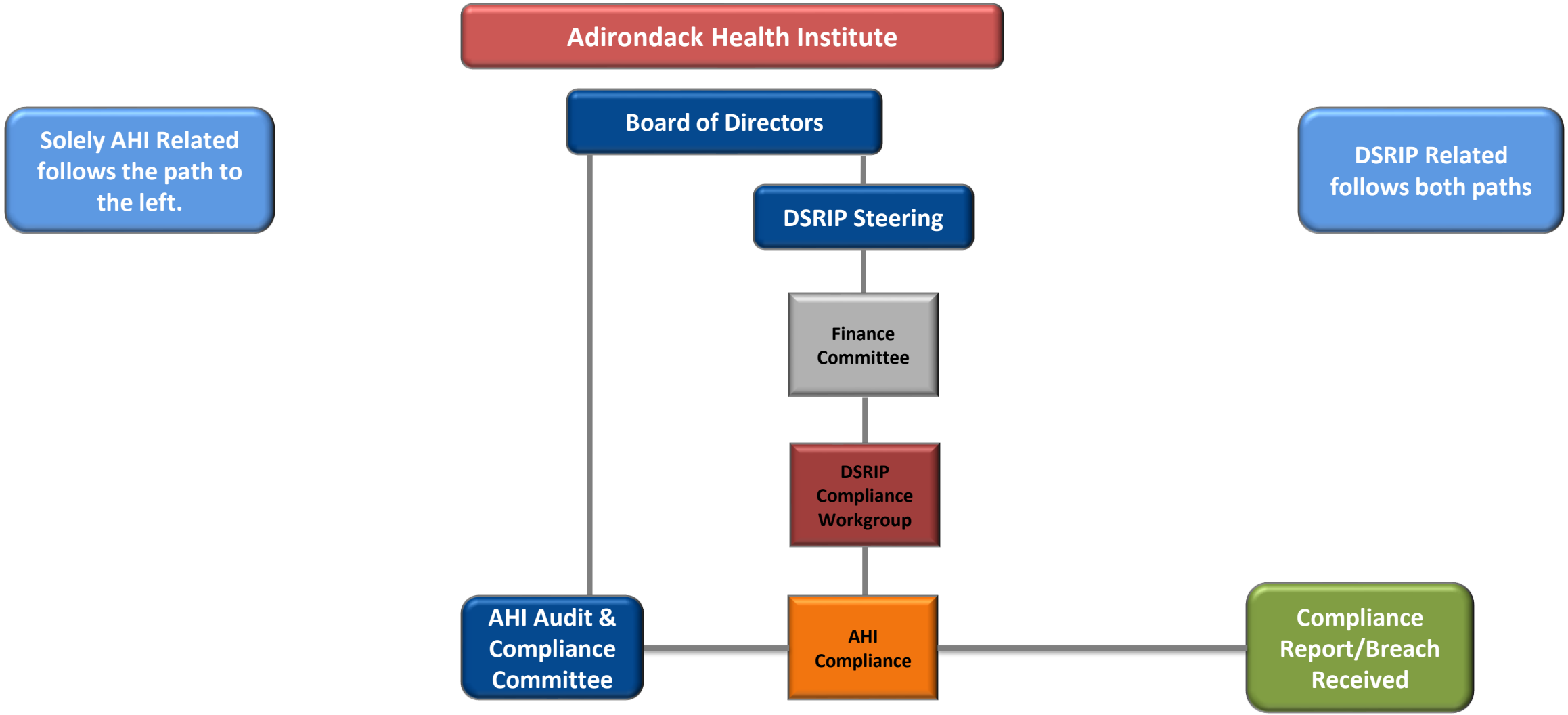
Differences Between Fraud, Waste and Abuse

Waste: Overutilization of services, or other practices that, directly or indirectly, result in unnecessary costs to the Medicare/Medicaid Program. Waste is generally not considered to be caused by criminally negligent actions but rather the misuse of resources.

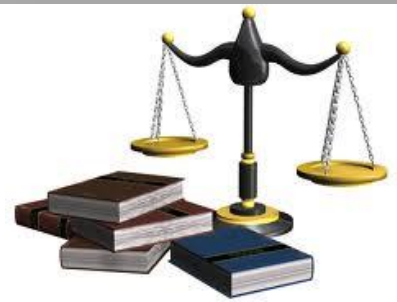
Abuse: Includes actions that may, directly or indirectly, result in unnecessary costs to the Medicare/Medicaid Program. Abuse involves payment for items or services when there is not legal entitlement to that payment and the provider has not knowingly and or/intentionally misrepresented facts to obtain payment.

There are differences between fraud, waste, and abuse. One of the primary differences is **intent and knowledge**. **Fraud** requires the person to have an intent to obtain payment and the knowledge that their actions are wrong. Waste and abuse may involve obtaining an improper payment, but does not require the same intent and knowledge.

Roadmap For Compliance Reporting



Laws and Regulations Related to Fraud, Waste, and Abuse



Criminal Health Care Fraud Statute ~ Statute: 18 U.S.C. §§ 1347, 1349

The False Claims Act ~ Statute: 31 U.S.C. §§ 3729–3733

The Anti-Kickback Statute ~ Statute: 42 U.S.C. § 1320a–7b(b), Safe Harbor Regulations: 42 C.F.R. § 1001.952

The Physician Self-Referral Law ~ Statute: 42 U.S.C. § 1395nn, Regulations: 42 C.F.R. §§ 411.350–.389

The Exclusion Authorities ~ Statutes: 42 U.S.C. §§ 1320a–7, 1320c–5, Regulations: 42 C.F.R. pts. 1001 (OIG) and 1002 (State agencies)

The Civil Monetary Penalties Law ~ Statute: 42 U.S.C. § 1320a–7a, Regulations: 42 C.F.R. pt. 1003

For more information on these laws, please visit: http://oig.hhs.gov/fraud/PhysicianEducation/01laws.asp
To review OIG enforcement actions, please visit: http://oig.hhs.gov/fraud/enforcementactions.asp

What is PHI? – Patient "Identifiers"

1. **Names**;
2. **Geographical subdivisions** smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code, if according to the current publicly available data from the Bureau of the Census: (1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
3. **All elements of dates** (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
4. **Phone numbers**;
5. **Fax numbers**;
6. **Electronic mail addresses**;
7. **Social Security numbers**;
8. **Medical record numbers**;
9. **Health plan beneficiary numbers**;
10. **Account numbers**;
11. **Certificate/license numbers**;
12. **Vehicle identifiers and serial number**s, including license plate numbers;
13. **Device identifiers** and serial numbers;
14. Web Universal Resource Locators (**URLs**);
15. Internet Protocol **(IP) address** numbers;
16. **Biometric identifiers**, including finger and voice prints;
17. Full face **photographic images** and any comparable images; and
18. **Any other unique identifying number, characteristic, or code** (note this does not mean the unique code assigned by the investigator to code the data)

Cyber Terrorism – Best Practice Reminders for Staff

- **Check for Confidential Content –** Before forwarding or replying to emails, check any attachments and the body of the email for sensitive data. Scroll all the way to the bottom of the email and check for confidential content (PHI, PII, or a combination of PHI and PII – SSN, CIN, credit card data, etc.)

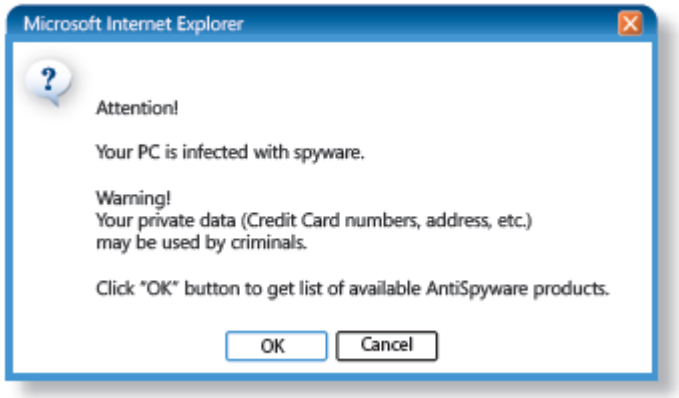
- **Links and Attachments –** Do not click on links or open attachments from Unknown senders. If you receive an email from a Known sender that looks out of the ordinary, do not open the attachment or click on the link.

- **Beware of Social Engineering Tactics:**

- Customized personal message text ("Dear John, ..." or "please review the attached invoice for...")
- Spoof (forge) the sender name so it appears to be from someone you know ("some-name@uiowa.edu")
- Make the message threatening ("your account will be closed unless you ...")
- Make the message look official from ("support@microsoft.com")
- Make the attachment look harmless ("my_vacation_pictures.php")

Cyber Terrorism – Best Practice Reminders Cont.

- **Manually Encrypt –** When sending sensitive data to authorized individuals outside AHI, manually encrypt the email.
- **Keep a Clean Machine –** Make sure to store sensitive data on a secure drive and not a local drive.
- **Firewall/Security Protections –** Never manually override any of your computer's firewall or security protections.
- **Avoid Clicking –** If you see a pop-up like this:



Avoid clicking on any of these buttons (OK, Cancel, etc). Instead, close the window by pressing CTRL and F4 on your keyboard.

Cyber Terrorism – Best Practice Reminders Cont.

- **Guard company data when you're on the go**

Treat all public Wi-Fi networks as a security risk.

- Choose the most secure option—it could include password-protection or encryption—even if you have to pay for it.
- Confirm the exact spelling of the wireless network you're connecting to— beware of clever (slightly misspelled) fakes, such as **www.micrsoft.com**.
- Encrypt all confidential data on smartphones, laptops, flash drives, and other portable devices in case they're lost or stolen.
- Never make financial and other sensitive transactions on any device over public wireless networks.
- Whenever possible, connect to a VPN.

Use flash drives carefully. Minimize the chance that you'll infect your company network with malware (be sure to follow your organization's media policy)**:**

- Don't put **any** unknown flash (or USB) drive into your computer (USB drives handed out at Expos).
- Whenever possible use Encrypted Flash Drives and don't open any unfamiliar files on your flash drive.

Cyber Terrorism – Best Practice Reminders Cont.

- **Verify –** Trust but verify.
- **Hover –** Before clicking on a link or a linkable item (photo, PDF, image), hover over it with your mouse to reveal the address. Make sure it is legitimate. If it appears to be suspicious, do not click.
- **Compare –** Compare a web address in a link with the actual address that is associated with the legitimate site. Look for changed letters or other variations.
- **Caution –** If something seems suspicious or too good to be true, always err on the side of caution.
- **Links –** Never use links in an email to connect to a site unless you are ABSOLUTELY SURE they are authentic. It is safer to type the URL directly into the browser.
- **Sharing Online –** Be careful what you share online. Personal information you share online could be used to target you (spear phishing).
- **Embedded Forms –** Never submit confidential information on forms embedded within email messages.
- **Social Networking –** Do not assume social networking sites are safe. Pictures, videos, invitations to games, applications, menus, and navigational elements can all be infected with malware.
- **Report –** Immediately report suspicious network activity and suspected phishing attacks (that are likely to trick co-workers) to your Compliance and/or IT Departments (and AHI Compliance when necessary).

Continuous On-Boarding and Annual Training

*Please remember that as rolled out with the 2017 DSRIP Compliance Training and with the 2017 General & DSRIP Compliance Training, your organization is required to use the training that you were assigned as continuous annual training, as well as on-boarding/new hire training.

You will be attesting to this completion on the Attestation for the 2018 DSRIP Compliance Training.

Additional Materials Provided

Annual Risk Assessment Policy	***Antitrust Policy***
AHI PPS Progressive Sanctions Policy	***Breach Notification Policy***
Code of Conduct with Board Governance Committee Addendum (COC/COI)	***Complaint Reporting and Customer Service Request Policy and Procedure***
Compliance Reporting and Response	***Confidentiality of Client Health Information Policy & Confidentiality Agreement***
Corporate Compliance Plan	***DSRIP Financial Sustainability Plan***
PPS Dispute Resolution Policy	***Security Policy - Network Security***
Written Information Security Policy (WISP)	***Attestation (for Organization-wide Training & Policy Review)***

http://www.ahihealth.org/ahipps/ahi-pps-policies-procedures/

Policy Tech Portal – For Use by Org's Compliance Individual

- Each partner organization will have one person who is able to access the policy management system.
  - This person will be the organization's responsible Compliance Contact.

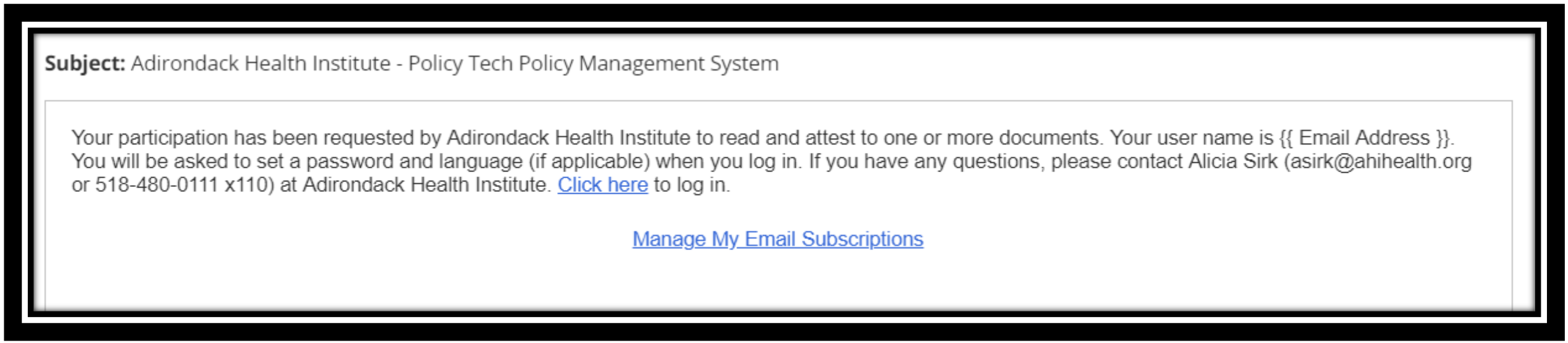
- You will receive a Welcome email, if you haven't already, with instructions on how to login.
- You will use this account to download (print and disseminate) policies for review by all those affected individuals to be trained at your organization.

- You will also use this system to Attest to policies and the training for your organization. Please be sure to not only mark policies read, but also complete any attached questionnaires or forms for each policy indicated. Policies that require a questionnaire and is not completed, but is marked as read, are considered incomplete.

- You should be able to use this system to return any documents electronically, that we require for DSRIP Compliance training.

- If you have any issues, please reach out to Alicia Sirk at asirk@ahihealth.org or 518-480-0111 x110.

Policy Tech Portal – Welcome Letter



Subject: Adirondack Health Institute - Policy Tech Policy Management System

Your participation has been requested by Adirondack Health Institute to read and attest to one or more documents. Your user name is {{ Email Address }}. You will be asked to set a password and language (if applicable) when you log in. If you have any questions, please contact Alicia Sirk (asirk@ahihealth.org or 518-480-0111 x110) at Adirondack Health Institute. Click here to log in.

Manage My Email Subscriptions

This is for use by the Organization's Compliance Contact only.

Alicia D. Sirk, MA, CHC, CHPC

Corporate Compliance and Privacy/Security Specialist

asirk@ahihealth.org

x110

Jeff Hiscox, BS, CHC

Chief Compliance Officer

jhiscox@ahihealth.org

x109

a·H·I Adirondack Health Institute