Adirondack Health Institute

Lead • Empower • Innovate

2017 General & DSRIP Compliance Training

PRESENTED BY:

Alicia Sirk, MA, CHC

Corporate Compliance and Privacy/Security Specialist

3/1/2017

What Is Compliance?

- ***Compliance*** means obeying the rules and regulations outlined by AHI Policy, by the New York State Department of Health (NYSDOH) & Office of Medicaid Inspector General (OMIG)

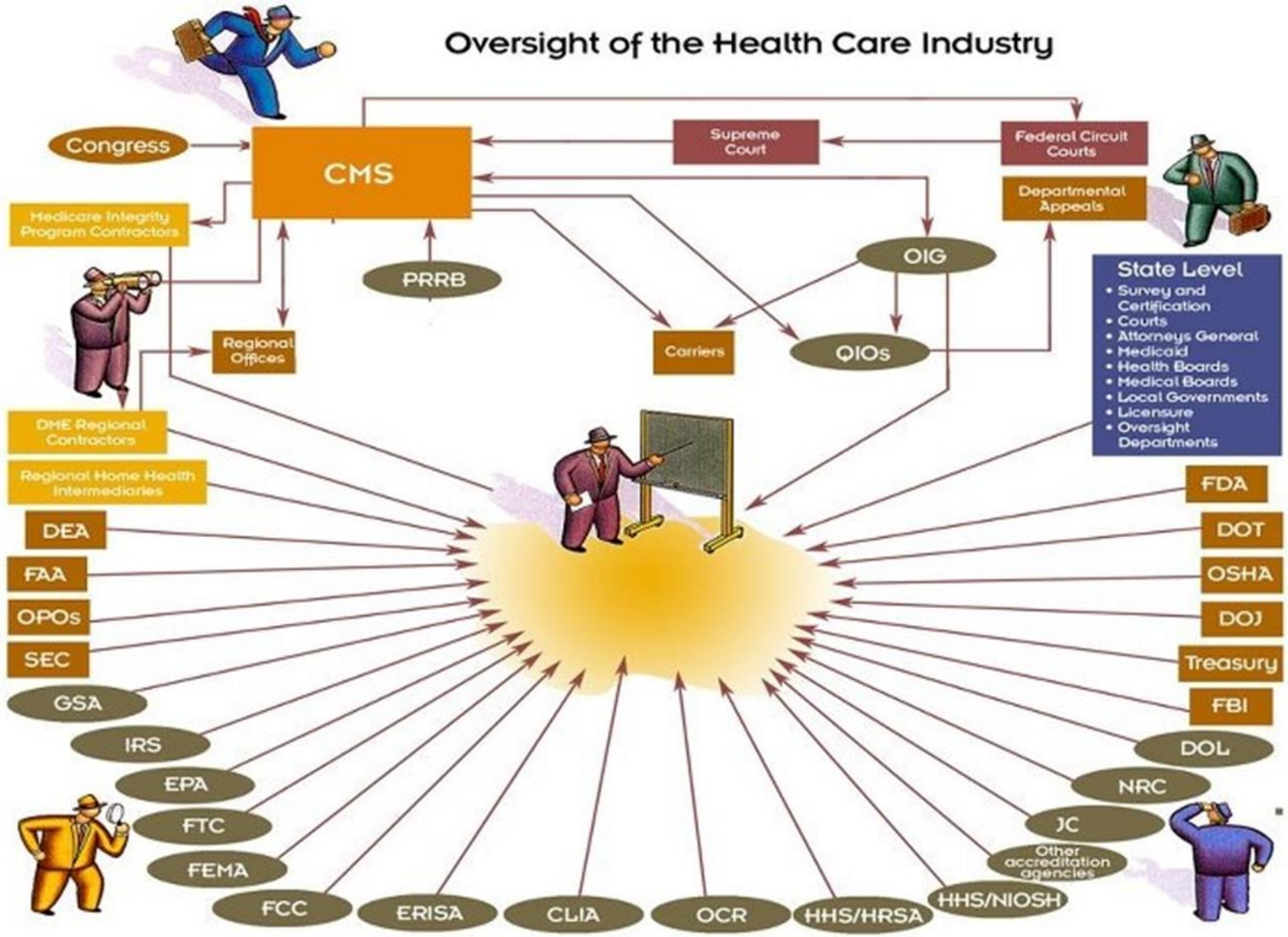
- An obligation to create a comprehensive Compliance Program that encompasses the New York Social Services Law Section 363-d (SSL 363-d) Title 18 of the New York Codes Rules and Regulations at Part 521 (Part 521).
  - Required by OMIG of providers that:
    - Are subject to Public Health Law A. 28 / 36 or Mental Hygiene Law A. 16 / A.31; *or*
    - Claim, order, bill, or receive more than $500,000 / 12 months from Medicaid;
  - Required by AHI PPS as part of your participation in DSRIP

Why is Compliance Important?

- Federal and state governments have created a ***vast number of laws and regulations*** that govern the business practices of health care organizations; including the actions of their management, staff, and contractors.

- The goal of these laws and regulations is to ***prevent fraud, waste and abuse*** and ***thereby protect consumers and government health care programs***.

- ***Failure to comply*** with applicable laws and regulations may result in ***civil and criminal liability*** of both the partner organization and the individual acting in noncompliance.


Oversight of the Health Care Industry
Congress
CMS
Supreme Court
Federal Circuit Courts
Departmental Appeals
Medicare Integrity Program Contractors
PRRB
OIG
State Level
• Survey and Certification
• Courts
• Attorneys General
• Medicaid
• Health Boards
• Medical Boards
• Local Governments
• Licensure
• Oversight Departments
Regional Offices
Carriers
QIOs
DME Regional Contractors
Regional Home Health Intermediaries
DEA
FAA
OPOs
SEC
GSA
IRS
EPA
FTC
FEMA
FCC
ERISA
CLIA
OCR
HHS/HRSA
HHS/NIOSH
Other accreditation agencies
JC
NRC
DOL
FBI
Treasury
DOJ
OSHA
DOT
FDA

Regulatory Compliance

The Centers for Medicare and Medicaid Services (CMS) requires a comprehensive plan to detect, prevent, and correct fraud, waste, and abuse (FWA) in the Medicare program. An element of the plan includes *effective* fraud, waste, and abuse **training and education**.

New York Compliance Program Requirements

- Condition of receiving Medicaid payments
- Annual certification that compliance program requirements have been met
- Required elements of an effective compliance program:
  1) **Written Policies and Procedures** (Compliance Plan and Code of Conduct - includes measures to detect, correct and prevent fraud, waste and abuse)
  2) **Designate Employee Vested with Responsibility** (Establishment of Audit & Compliance Committee and a Regional Compliance Workgroup)
  3) **Training and Education** (New hire orientation, Annual in-service, Response to compliance risk areas, Response to changes in regulations)
  4) **Communication Lines to the Responsible Compliance Position**
  5) **Disciplinary Policies to Encourage Good Faith Participation** (Enforcement of Standards)
  6) **System for Routine Identification of Compliance Risk Areas** (Procedures for Internal Monitoring and Auditing)
  7) **System for Responding to Compliance Issues** (Prompt response to detected offenses)
  8) **Policy of Non-Intimidation and Non-Retaliation**
  9) **HIPAA (Privacy & Security)**

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

Criminal Health Care Fraud Statute

- Prohibits knowingly and willfully executing, or attempting to execute, a scheme or artifice in connection with the delivery of or payment for health care benefits, items, or services to either:
  - Defraud any health care benefit program
  - Obtain (by means of false or fraudulent pretenses, representations, or promises) any of the money or property owned by, or under the control of, any health care benefit program

Example: Several doctors and clinics conspire in a coordinated scheme to defraud Medicare by submitting claims for power wheelchairs that were not medically necessary.

***Penalties for violating the Criminal Health Care Fraud Statute may include fines, imprisonment, or both.**

False Claims Act (31 U.S.C. § 3729-3733)

The False Claims Act (FCA) imposes civil liabilities on organizations and individuals that knowingly make false claims for payment to the government, including for health care programs such as Medicare or Medicaid. The FCA applies to hospitals, providers, beneficiaries, and health plans doing business with the federal government as well as billing companies, contractors, and other persons or entities connected with the submission of claims to the government.

Prohibits:

- Presenting a false claim for payment or approval;
- Making or using a false record or statement in support of a false claim;
- Conspiring to violate the False Claims Act;
- Falsely certifying the type/amount of property to be used by the Government;
- Certifying receipt of property without knowing if it's true;
- Buying property from an unauthorized Government officer; and
- Knowingly concealing or knowingly and improperly avoiding or decreasing an obligation to pay the Government.

False Claims Act (Penalties)

- Anyone who violates the FCA is liable for **civil penalty** of not less than $10,781 and not more than $21,563 per claim (eff 8/1/16), plus three times the amount of the damages the government sustains. The government may also place violators on **EXCLUSIONS LISTS**.
- Intentional submission of a false claim is subject to federal **criminal enforcement** and may also be liable to the United States government for the costs of civil action brought to recover any penalties or damages.
- The government relies heavily on the federal and state FCA to prosecute billing fraud. The FCA authorizes *qui tam* actions (1) the ability to sue, on behalf of the government, persons or entities who knowingly have presented the government with false or fraudulent claims; and awards to *qui tam* plaintiffs (2) a share in any proceeds ultimately recovered as a result of the suit.

**The FCA includes provisions to discourage employers from retaliating against employees for initiating *qui tam* lawsuits.

False Claims Act (NY) NYS SSL § 145-b

The New York False Claims Act is triggered by claims for payment submitted to the state and its agencies. The New York False Claims Act is very similar to the Federal FCA in terms of the types of acts that give rise to liability.

- **NY State makes it unlawful to knowingly make a false statement or representation to attempt to obtain Medicaid payments for services or supplies furnished under the New York State Medical Assistance Program.**
- **Under NY State Penal Law it is a crime to commit "health care fraud".**
- **Civil Prosecution and Penalties: $6,000-$12,000 per claim and recoverable damages between two and three times the value of the amount falsely received.**

The Office of Inspector General's self-disclosure protocol allows providers to conduct their own investigations, take appropriate corrective measures, calculate damages and submit the findings that involve more serious problems than just simple errors to the agency.

AHI/AHIPPS and each of its workforce members will fully comply with the False Claims Act, whistle blower statutes, and all reporting procedures. Any AHI workforce member found to be in violation of the False Claims Act will face sanctions up-to termination of employment, affiliation, or contract with AHI/AHIPPS, in accordance with general AHI disciplinary policies.

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

- Individuals who report problems or concerns in good faith will be protected from retaliation, retribution or harassment.
- Employees who engage in retribution, harassment or any other type of retaliatory action will be subject to disciplinary action up to and including termination of employment.
- An employee who believes that he or she has been discharged, demoted, or otherwise discriminated against contrary to whistleblower protections 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.

NYS Protections

- **New York Labor Law §741**: an employer may not take retaliatory action against an employee who disclosed information about their employer to a regulatory agency.

- **New York Labor Law §740**: Protected disclosures are those that an employer is in violation of a law that may constitute fraud under Penal Law §177. Person has knowledge of false claim activity.

- **Provide protection to *qui tam* (private individuals)** who are discharged, demoted, suspended, harassed or any other manner discriminated against in the terms and conditions of their employment.

Anti-Kickback Statute (AKS)

Makes it a crime to knowingly and willfully offer, pay, solicit, or receive **any** remuneration directly or indirectly to induce or reward referrals of items or services reimbursable by a Federal health care program.

Example: A provider receives cash or below fair market value rent for medical office space in exchange for referrals.

***Penalties: Civil penalties may include penalties of up to $73,588 (in 2016) per kickback plus three times the amount of the kickback. Criminal penalties may include fines, imprisonment, or both.**

(If certain types of arrangements satisfy regulatory Safe Harbors, they may not violate the AKS.)

Stark Law

Prohibits a physician from making a referral for certain Designated Health Services payable by Medicare or Medicaid to an entity in which the physician (or an immediate family member) has an ownership/investment interest or with which he or she has a compensation arrangement, unless an Exception applies.

Example: A provider refers a beneficiary for a designated health service to a business in which the provider has an investment interest.

***Penalties for physicians who violate the Stark Law may include fines, penalties up to $23,863 (in 2016) for each service, repayment of claims, and potential exclusion from all Federal health care programs.**

Exclusions

- Excluded providers may not participate in Federal or State health care programs for a designated period.
- An excluded provider may not bill these health care programs (including, but not limited to, Medicare & Medicaid) for services he or she orders or performs. Additionally, an employer or a group practice may not bill for an excluded provider's services.
- At the end of an exclusion period, an excluded provider must seek reinstatement; reinstatement is not automatic.
- The OIG maintains a list of excluded parties called the List of Excluded Individuals/Entities (LEIE) and OMIG maintains the List of Restricted and Excluded Providers. AHI checks these databases, among others, prior to hire and on a continuous basis to ensure that providers, employees, and others associated with AHI/AHIPPS are not excluded from program participation.

Exclusions (cont.)

- OIG must exclude any providers and suppliers convicted of any of the following:
  - Medicare fraud and any other offenses related to the delivery of items or services under Medicare
  - Patient abuse or neglect
  - Felony convictions for other health care-related fraud, theft, or other financial misconduct
  - Felony convictions for unlawful manufacture, distribution, prescription, or dispensing of controlled substances
- OIG also has discretion exclude on other grounds, including:
  - Misdemeanor convictions related to health care fraud other than Medicare or Medicaid fraud, or misdemeanor convictions in connection with the unlawful manufacture, distribution, prescription, or dispensing of controlled substances
  - Suspension, revocation, or surrender of a license to provide health care for reasons bearing on professional competence, professional performance, or financial integrity
  - Providing unnecessary or substandard services; submitting false or fraudulent claims
  - Engaging in unlawful kickback arrangements
  - Defaulting on health education loan or scholarship obligations

HIPAA Privacy and Security

Emphasizing the Importance of Protecting Patient Information

Privacy – Protection for the privacy of Protected Health Information

- **Protected Health Information** (PHI) is individually identifiable health information which may either be verbal or written. It can be a past, a present or a future physical or mental health condition.

Security – Protection for the security of electronic Protected Health Information (e-PHI)

- **Electronic Protected Health Information**
- (e-PHI) is computer-based patient health information that is **used, created, stored, received or transmitted** using any type of electronic information resource.

Difference Identity Theft vs Privacy Breach

- Identity Theft
  - Stealing Personally Identifiable Data
  - Purpose – Enable Stealing $$$ via Identity Fraud
- Privacy Breach
  - Learning Embarrassing Personal Information
  - Purpose is Rarely $$$
  - Purpose – Enable Ridicule or Blackmail

Problem – INSIDER Identity Theft/Privacy Breach

Insiders, Not Outsiders, Accounted For:

- 71% of Customer Records Compromised or Stolen
- 63% of Employee Records Compromised or Stolen

How does this happen??

- Snooping, Theft, Phishing/Hacking (a hacker steals credentials of employees), and “selling” info

"Organizations who have good insider threat and data protection programs will be around in 10 years, **and those that don't -- won't”** - *Patrick Reidy - FBI Chief Information Security Officer*

Data Theft Federal Legislation

- Recent legislation cases affect class action suits, fines and penalties for privacy breaches and identity data thefts by insiders.
- Class Action by Customers/Patients/Clients:
  - $3 million settlement in FL even though **NO Proof of Harm.**
  - WV Supreme Court OK's suit with **NO Proof of Injury.**
  - $4 Billion cuit of CA health care firm would have gone to trial if "**proof unauthorized person accessed stolen material.**"
- FTC Now Involved:
  - US Court of Appeals for 3rd Circuit on 8/24/15 AFFIRMED **FTC** Jurisdiction on Data Theft
    - Health care will face BOTH **HHS** and **FTC** over single loss
  - Settled with Health Care Firm, citing:

"Not using readily-available measures to prevent and detect unauthorized access to personal information."

Why is Identity Theft Growing??

- Organizations store more Identity Data
- More Employees Need/Given Access to Identity Data
- Identity Data is More Valuable than Credit Card Data
  - Medical Record = $50.00
  - Credit Card = $1.50
- Fraud Using Stolen Identity Data is Lucrative
  - Stolen Identity Refund Fraud (SIRF) = $21 Billion 2012-2017
    - -$2.1 Million for a Single Tax Refund
    - -34% of all Reported Identity Fraud
  - Credit Card (17%), Bank (8%), Loan (4%)

HIPAA Privacy ~ *a set of national standards for the use and disclosure of individually identifiable health information or PHI*

- Notice of Privacy Practices – required to provide at initial appointment/visit, post in a public location, and make available upon request.

- Individual Rights under the Privacy Rule
  - Notice of Privacy Practices
  - Access to Health Information
  - Right to Amendment of PHI
  - Right to Request Restrictions
  - Right to Request Confidential Communications
  - Right to Request an Accounting of Disclosures
  - Right to file a Complaint with the Privacy [Compliance] Officer as well as US Dept. of HHS regarding AHI privacy practices or concerns with breach of confidentiality

HIPAA Security Safeguards

1. Administrative safeguards
   - Security management
   - Staff training
   - Information access management
   - Contingency plan for emergencies

2. Physical safeguards
   - Facility access controls such as locks and alarms
   - Workstation security measures
   - Workstation use policies

3. Technical safeguards
   - Access controls to restrict access to PHI by authorized personnel
   - Audit controls to monitor activity
   - Integrity controls to prevent improper alteration or destruction
   - Transmission security

Examples of HIPAA Breach ~

Loss, theft, or other impermissible uses or disclosures of unsecured PHI

Breach - the acquisition, access, use, or disclosure of Protected Health Information in a manner not permitted under HIPAA, which compromises the security or privacy of the protected health information.

- A document is sent/emailed/faxed to the wrong individual which is opened by the recipient; a document is left on a printer.
- An Excel file with PHI records is emailed to the wrong person.
- An employee accidentally gives a form to the wrong client/patient.
- Lost or stolen laptops, smartphones, flash drives, etc…
- Losing a document, bill, or medical record with PHI on it.
- Employee looking (snooping) in a client/patient record – not related to direct client/patient care or quality review.
- Sharing information you learned about a client/patient – not related to direct client/patient care or quality review.
- Reviewing census information just to see who is in a program/admitted into a facility.
- Any record review not related to your job, direct client/patient care, or as part of quality review.

Fines and Penalties for HIPAA Violations

HIPAA Violation	Minimum Penalty	Maximum Penalty
Individual did not know (and by exercising reasonable diligence would not have known) that he/she violated HIPAA	$100 per violation, with an annual maximum of $25,000 for repeat violations (Note: maximum that can be imposed by State Attorneys General regardless of the type of violation)	$50,000 per violation, with an annual maximum of $1.5 million
HIPAA violation due to reasonable cause and not due to willful neglect	$1,000 per violation, with an annual maximum of $100,000 for repeat violations	$50,000 per violation, with an annual maximum of $1.5 million
HIPAA violation due to willful neglect but violation is corrected within the required time period	$10,000 per violation, with an annual maximum of $250,000 for repeat violations	$50,000 per violation, with an annual maximum of $1.5 million
HIPAA violation is due to willful neglect and is not corrected	$50,000 per violation, with an annual maximum of $1.5 million	$50,000 per violation, with an annual maximum of $1.5 million

Adirondack Health Institute

Lead • Empower • Innovate

2017 DSRIP Compliance Training

PRESENTED BY:

Alicia Sirk, MA, CHC

Corporate Compliance and Privacy/Security Specialist

3/1/2017

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 and partner organizations.
- **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.

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.

Corporate Compliance Program Applicability

- The Corporate Compliance Program applies to all **Affected Individuals**:
  - Members of the Board
  - Executives
  - Medical Staff
  - Employees
  - Volunteers
  - Students & Interns
  - Vendors
  - Agents
  - Independent Contractors

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.

The OMIG's September 2015 DSRIP Compliance Guidance: Elements of a DSRIP Compliance Program

1. **PPS Leads must have policies/procedures specifically relating to DSRIP issues. These must identify how PPS Partners can communicate issues to the PPS Compliance Officer.**
2. **PPS Compliance Officer must be an employee of PPS Lead, reporting to senior leadership and providing reports to the governing body.**
3. **PPS Lead is responsible for compliance training. PPS Lead doesn't have to provide training itself to Partners: can provide materials, get confirmation that the Partners provided training.**
4. **PPS Lead must have established process of reporting compliance issues to Compliance Officer, including by an anonymous/confidential method.**
5. **PPS Lead needs disciplinary policies and procedures to encourage good faith participation in the PPS compliance program by all affected individuals. These should be communicated in training and PPS Leads should "support implementation…throughout the [PPS] network."**
6. **The Lead must develop/implement system for routine identification of compliance risk areas specific to provider type. Risk areas include PPS Partners' DSRIP performance, which should be monitored.**
7. **PPS Lead must have system for responding to compliance issues like the Lead's internal misuse of DSRIP funds or a Partner's false statements made to obtain funds. There must be a system for corrective action. PPS Lead must work with Partners to support adherence to this requirement.**
8. **The Lead must have policy of non-intimidation and non-retaliation, support Partners' compliance with this requirement.**

Selections from September 2015 OMIG Guidance

- "PPS Leads… must…take all reasonable steps to ensure that Medicaid funds distributed as part of the DSRIP program are not connected with fraud, waste or abuse. It is reasonable for a PPS Lead to consider its [PPS Partners'] program integrity systems when [doing so]."
- "PPS Leads can focus their compliance program risk assessments on those risks specifically associated with the current phase of the DSRIP program and payments made pursuant to it."
- "PPS Leads are not responsible for network providers' individual compliance programs that may be required in connection with their status as a serving provider. Likewise PPS Leads cannot be responsible for how network providers use their respective DSRIP distributions, but PPS Leads must have adequate processes in place…to be able to identify when network providers obtain DSRIP distributions in a way that is inconsistent with approved DSRIP project plans."
- Full text of the OMIG Guidance at https://www.omig.ny.gov/images/stories/compliance_alerts/20150901_DSRIP_CompGuidance_2015-01_Rev.pdf.

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/
- 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.	

Discipline and Sanctioning

- PPS Leads must have disciplinary policies to encourage good faith participation in the PPS compliance program by all affected individuals [Element 5.]
- Roles and responsibilities:
  - PPS Leads are responsible for disciplining their own staff.
  - PPS Partners must comply with this requirement with respect to their staff. OMIG guidance states that 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 Articles VIII, IX, and X of AHI Master Participation Agreement.

Risk Assessment, Auditing and Monitoring

- PPS Lead is required to develop/implement system for routine identification of compliance risk areas [Element 6.]
- This process will inform auditing and monitoring activities.
- Auditing is a "formal, systematic and disciplined approach designed to evaluate and improve the effectiveness of processes and related controls." An audit is usually conducted by an objective professional independent of the process or function.
- Monitoring is an "on-going process usually directed by management to ensure processes are working as intended." Monitoring is usually conducted by operations personnel responsible for the process or function.

PPS Leads must conduct or direct auditing or monitoring of their own DSRIP-related activities and those of their PPS Partners. This may entail review of books, records and other information made available by the PPS Partner to the Lead. [Note to draft: may want to cite to master services agreement.] (See also Annual Risk Assessment Policy.)

Quotations above from 2004 white paper on the definitions of auditing and monitoring by a joint task force of the Association of Healthcare Internal Auditors and the Health Care Compliance Association.
https://www.ahia.org/assets/Uploads/pdfUpload/WhitePapers/DefiningAuditingAndMonitoring.pdf

Responding to Compliance Issues

- AHI PPS Lead (AHI) must have system for responding to compliance issues like the Lead's internal misuse of DSRIP funds or a Partner's false statements made to obtain funds. There must be a system for corrective action. PPS Lead must work with partners to support adherence to this requirement [Element 7].
- AHI PPS Lead will directly review or investigate issues or delegate that duty to the involved PPS Partner, which would then be responsible for reporting results back to Lead.

See Article IV, Article VIII and Article XIII of AHI Master Participation Agreement.

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.

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 Officer:***

- **Anonymous Compliance Hotline**: 844-386-2242 (externally)
- **Chief 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.*****

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 Corporate Compliance Officer. Anyone who makes a good faith report to their immediate supervisor or the Corporate Compliance Officer, 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 Officer, 101 Ridge Street, Glens Falls, NY 12801.

- Compliance report forms may be completed anonymously and training on location of forms will be provided to all employees, executives, interns, volunteers, and governing body members during compliance training. Additionally, forms will be provided to contractors and agents of AHI and will be made available on AHI's website.

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 corporate compliance violation. If retaliation occurs, it should be reported immediately to the Compliance Officer, the CEO, or the Board of Directors.

- AHI expects that all PPS Partners will comply with the compliance plan, including the requirements of monitoring, auditing, self-disclosure, and reporting and in 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 Chief Compliance Officer 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.

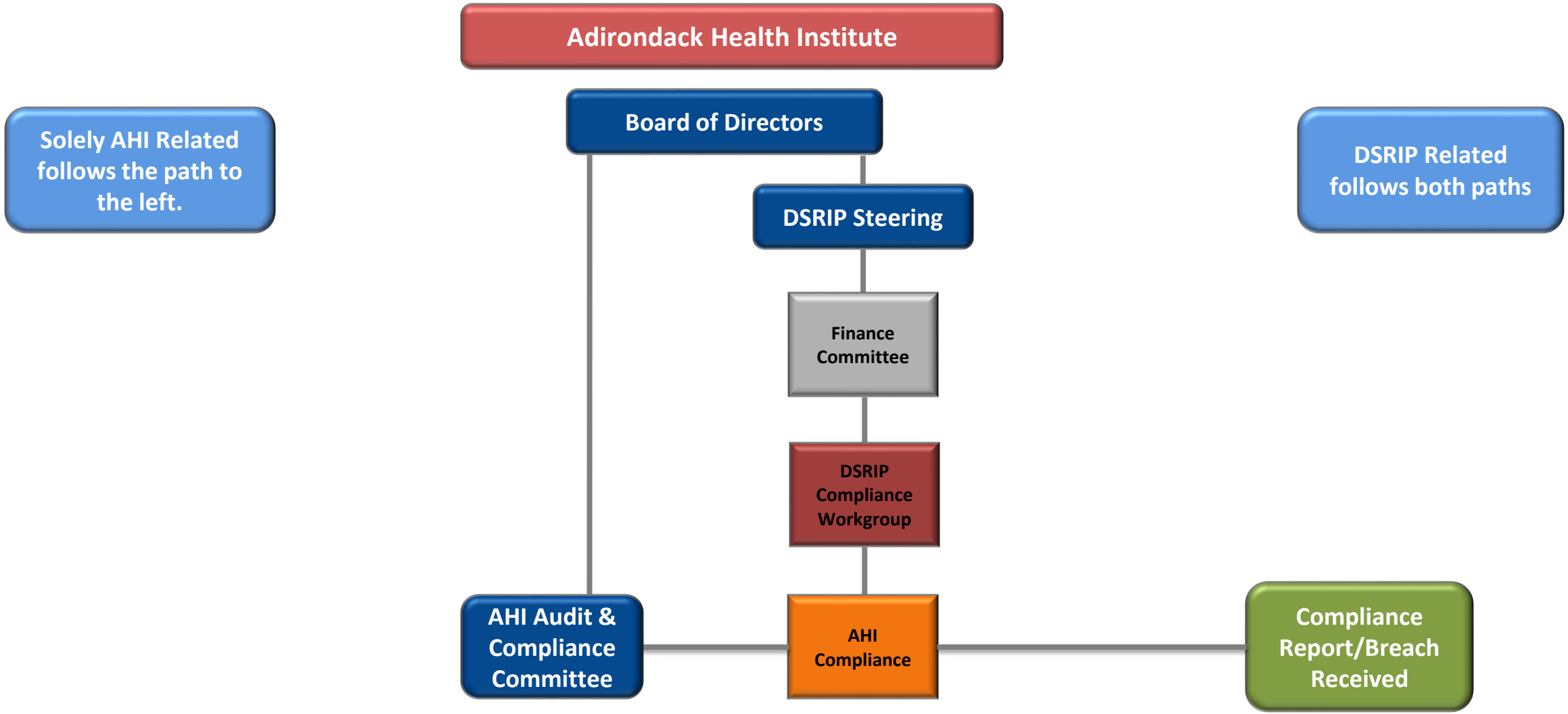
Differences Between Fraud, Waste and Abuse

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



Special issues to watch for

- Laws and Regulations related to Fraud, Waste, and Abuse
- Antitrust (see policies)
- Data privacy and security

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)

Additional Materials Provided

Annual Risk Assessment Policy	***Antitrust Policy***
AHI PPS Dispute Resolution Policy	***AHI PPS Progressive Sanctions Policy***
Breach Notification Policy	***Code of Conduct/Conflict of Interest***
Complaint Reporting and Customer Service Request Policy	***Compliance Reporting and Response***
Corporate Compliance Plan	***DSRIP Financial Sustainability Plan***
Security Policy - Network Security	***Written Information Security Policy (WISP)***
Attestation	

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

Jeff Hiscox, BS

Chief Compliance Officer

jhiscox@ahihealth.org

x109

Alicia D. Sirk, MA, CHC

Corporate Compliance and Privacy/Security Specialist

asirk@ahihealth.org

x110

a·H·I Adirondack Health Institute