

Policy and Procedure		
SUBJECT: Disciplinary Standards- First Tier, Downstream and Related Entities (FDRs)	DEPARTMENT: Regulatory Compliance, Risk Management and Government Affairs	
ORIGINAL EFFECTIVE DATE: 09/12	DATE(S) REVIEWED/REVISED: 03/13, 03/14, 12/15, 09/16, 12/17, 09/18, 05/19, 04/20, 04/21, 06/22, 03/23, 04/24, 05/25	
APPROVED BY: Chief Compliance and Risk Officer	NUMBER: RA 67	PAGE: 1 of 5

SCOPE:

Providence Health Plan and Providence Health Assurance as applicable (referred to individually as “Company” and collectively as “Companies”).

APPLIES TO:

Fully Insured			Self-Insured	Medicare	Medicaid
Individual	Small Group	Large Group			
<input type="checkbox"/> Oregon On Exchange	<input type="checkbox"/> Oregon On Exchange (SHOP)	<input type="checkbox"/> Oregon	<input type="checkbox"/> ASO	<input checked="" type="checkbox"/> Medicare Advantage	<input type="checkbox"/> Medicaid
<input type="checkbox"/> Oregon Off Exchange	<input type="checkbox"/> Oregon Off Exchange (SHOP)	<input type="checkbox"/> Washington	<input type="checkbox"/> PBM	<input type="checkbox"/> Medicare Supplement	
<input type="checkbox"/> Washington Off Exchange				<input checked="" type="checkbox"/> Medicare Advantage – D-SNP	
<input type="checkbox"/> APPLIES TO ALL ABOVE LINES OF BUSINESS					

POLICY:

Medicare Advantage Plans is committed to monitoring its first-tier, downstream, and related entities (FDRs) for compliance with Companies and any applicable CMS/Federal regulations. When an FDR is found to be out of compliance with these regulations, the FDR will be subject to corrective action as deemed appropriate for the nature of the violation. Company clearly publicizes disciplinary standards for all FDRs on the FDR website.

DEFINITIONS:

1. **“Work Plan”** is a written document to be provided to the Delegated Entity to correct any minor issues of non-compliance. The Delegated Entity is required to respond.
2. **“Corrective Action Plan”** is a formal written document that requires the delegate to provide a remediation plan with a strict remediation deadline. This document is tracked by Company to ensure full remediation and compliance from the FDR. A Corrective Action Plan includes, but is

Policy and Procedure		
SUBJECT: Disciplinary Standards- First Tier, Downstream and Related Entities (FDRs)	DEPARTMENT: Regulatory Compliance, Risk Management and Government Affairs	
ORIGINAL EFFECTIVE DATE: 09/12	DATE(S) REVIEWED/REVISED: 03/13, 03/14, 12/15, 09/16, 12/17, 09/18, 05/19, 04/20, 04/21, 06/22, 03/23, 04/24, 05/25	
APPROVED BY: Chief Compliance and Risk Officer	NUMBER: RA 67	PAGE: 2 of 5

not limited to: counseling, re-education or training; verbal or written warnings, corrective action and/or termination of the FDR relationship.

3. **Providence Compliance Program PHP-PHA** is Company's formal program that fully describes Company's commitment to comply with all CMS/Federal guidelines and regulations. FDR means First Tier, Downstream or Related Entity. **"First Tier Entity"** is any party that enters into a written arrangement, acceptable to CMS, with Company to provide administrative services or health care services to a Medicare eligible individual under the MA program or Part D program. **"Downstream Entity"** is any party that enters into a written arrangement, acceptable to CMS, with persons or entities involved with the MA benefit or Part D benefit, below the level of the arrangement between Company's and a First Tier Entity. These written arrangements continue down to the level of the ultimate provider of both health and administrative services. **"Related Entity"** means any entity that is related to Company by common ownership or control and:
 - (1) Performs some of Companies management functions under contract or delegation;
 - (2) Furnishes services to Medicare enrollees under an oral or written agreement; or
 - (3) Leases real property or sells materials to Company at a cost of more than \$2,500 during a contract period.

PROCEDURE:

FDR Responsibilities:

1. **Compliance.** FDRs must comply with Company's Compliance Policies, PHP/PHA Standards of Conduct, FDR Delegation Agreement and/or contract, as well as Code of Conduct Policies and all applicable laws and regulations.
2. **Training.** FDRs must complete Compliance and Fraud, Waste, and Abuse training and attest to Company that training is complete. To fulfill the FDR's training requirement, the Medicare Compliance team will allow FDR's to complete Company's training or their own general compliance and Fraud, Waste and Abuse training. All training and education is reviewed and overseen by Company.
3. **Reporting.** FDRs must immediately report any potential non-compliance violations, including unethical or illegal behavior. There are multiple ways that an FDR may report potential non-compliance issues/concerns. It may be reported through routine auditing and monitoring, contacting the Medicare Delegation Program Consultant directly, filling out the electronic webform on the FDR webpage, or by filling out the potential non-compliance external referral pdf form and sending it to Company via mail .
4. **Non-retaliation.** Company maintains a policy of non-intimidation and non-retaliation against FDRs reporting a potential compliance concern.

Policy and Procedure		
SUBJECT: Disciplinary Standards- First Tier, Downstream and Related Entities (FDRs)	DEPARTMENT: Regulatory Compliance, Risk Management and Government Affairs	
ORIGINAL EFFECTIVE DATE: 09/12	DATE(S) REVIEWED/REVISED: 03/13, 03/14, 12/15, 09/16, 12/17, 09/18, 05/19, 04/20, 04/21, 06/22, 03/23, 04/24, 05/25	
APPROVED BY: Chief Compliance and Risk Officer	NUMBER: RA 67	PAGE: 3 of 5

5. Investigations. Company will thoroughly research any allegation of potential Medicare non-compliance or fraud, waste and abuse. FDRs shall assist in the resolution of reported issues as needed.

If it is found that an FDR is not meeting Company's compliance expectations, applicable laws and regulations or is in violation of the Providence Code of Conduct or the PHP/PHA Standards of Conduct, appropriate action will be taken, including but not limited to disciplinary actions and reporting of the conduct to the appropriate regulatory agency or law enforcement.

Company expects all FDRs to notify Company immediately when there has been unethical or non-compliant behavior. The FDR will also ensure that disciplinary action is taken as appropriate to the seriousness of the violation. Disciplinary action should be fair and consistently administered and imposed within a reasonable timeframe.

Company has identified a list of prohibited conduct and potential disciplinary actions that may be applied in response to a violation of compliance with applicable laws, regulations, Providence Compliance Program PHP-PHA and Standards of Conduct. The list of prohibited conduct serves as an example and is not representative of every situation.

Guidelines for Compliance Actions:

Level One - Unintentional Violation or Carelessness: A Level One violation occurs when a workforce member unintentionally accesses, reviews or discloses confidential information to anyone without a legitimate need to know. Examples of Level One violations include, but are not limited to:

- Inadvertently e-mailing or faxing PHI or other confidential information to the wrong person
- Failing to use secure e-mail when appropriate
- Discussion of patient information in a public area
- Failure to protect medical records or other PHI or ePHI
- Failing to lock computer screen when workstation is left unattended
- Failure to shut down laptops correctly with the result that encryption is not enabled
- Leaving more than the minimum required PHI on an answering machine and
- Careless handling of usernames and passwords, such as leaving sticky notes with passwords written on them on or near a computer or door keypad

Level One violation may be treated as a Level Two or Level Three violation depending on the magnitude of risk created, prior violations or corrective actions imposed on the workforce member for any reason, and/or when the workforce member has received training relating to confidential information.

Policy and Procedure		
SUBJECT: Disciplinary Standards- First Tier, Downstream and Related Entities (FDRs)	DEPARTMENT: Regulatory Compliance, Risk Management and Government Affairs	
ORIGINAL EFFECTIVE DATE: 09/12	DATE(S) REVIEWED/REVISED: 03/13, 03/14, 12/15, 09/16, 12/17, 09/18, 05/19, 04/20, 04/21, 06/22, 03/23, 04/24, 05/25	
APPROVED BY: Chief Compliance and Risk Officer	NUMBER: RA 67	PAGE: 4 of 5

Level Two - Intentional Violation or Curiosity/Concern: A Level Two violation occurs when a workforce member intentionally accesses, reviews, or discloses confidential information in an unauthorized manner or for unauthorized purposes, but for reasons unrelated to personal gain.

Examples of Level Two violations include but are not limited to:

- Looking up personal information such as birth dates or addresses of friends or relatives
- Sharing a computer password with another person or group
- Failure to follow device and media controls standards
- Accessing and reviewing a patient's record, including their own or that of a family member, when there is no job-related need to access
- Sharing patient or employee information with any individual who does not have a legitimate need to know
- Failure to complete required education programs
- Misuse of information systems in violation of Providence St. Joseph Health Policy-PSJH-CYBR- 950, Information Security Management
- Repeated incidents of Level One violations

A Level Two violation may be treated as a Level Three violation depending on the magnitude of risk created, prior violations or corrective action imposed on the workforce member for any reason, and/or when the workforce member has received training relating to confidential information.

Level Three - Violation for Personal Gain or Malice: A Level Three violation occurs when a workforce member accesses, reviews, or discloses confidential information for personal or monetary gain or with malice. Personal gain or malice includes intentional wrongful actions without justification. In almost all cases, Level Three violations will result in termination of employment. Examples of Level Three violations include but are not limited to:

- Selling patient or employee social security numbers or credit card numbers
- Falsifying or altering patient information
- Obtaining PHI under false representation
- Using confidential information to harass or intimidate other individuals, either internal or external to Company
- Misuse of confidential company information for personal gain or malice
- Deliberately compromising electronic information security measures
- Gross negligence in handling confidential information
- Subverting network controls – escalating privileges without authorization to do so; and/or
- Repeated Level One or Two violations

Policy and Procedure	
SUBJECT: Disciplinary Standards- First Tier, Downstream and Related Entities (FDRs)	DEPARTMENT: Regulatory Compliance, Risk Management and Government Affairs
ORIGINAL EFFECTIVE DATE: 09/12	DATE(S) REVIEWED/REVISED: 03/13, 03/14, 12/15, 09/16, 12/17, 09/18, 05/19, 04/20, 04/21, 06/22, 03/23, 04/24, 05/25
APPROVED BY: Chief Compliance and Risk Officer	NUMBER: RA 67 PAGE: 5 of 5

Potential Action Steps:

1. Retraining and re-evaluation
2. Discussion of policy and procedures
3. Written warning and acknowledgment of consequences of subsequent infractions
4. Suspension or termination of contract if warranted

The above serves as a guideline for Company. The compliance/disciplinary action will depend on the findings discovered through investigation.

REFERENCES:

CMS Managed Care Manual Chapters 9 and 21 – Compliance Program Requirements
 PHP/PHA Standards of Conduct
 Providence St. Joseph Health Policies PSJH-CPP-736 Compliance Hotline Policy, PSJH-CPP-735 Investigations Policy, PSJH-CPP-733 Non-Retaliation, PSJH-CYBR-950 Information Security Management