


<p><b>DEPARTMENT:</b> Compliance</p> <p><b>POLICY TITLE:</b> CMP20 Sanctions for HIPAA Violations</p>		
<p><b>REVIEWED BY:</b> AZPC Compliance Officer</p>	<p><b>REVIEW DATE:</b> 11/08/2019</p>	<p><b>EFFECTIVE DATE:</b> 12/01/2019</p>
<p><b>APPROVED BY:</b> Compliance Committee</p>	<p><b>APPROVAL DATE:</b> 11/11/2019</p>	

**PURPOSE:**

To ensure that Arizona Priority Care (AZPC) defines clear and appropriate sanctions for employees, volunteers, business associates and other members of the workforce who fail to comply with HIPAA policies and procedures.

**POLICY:**

It is AZPC’s policy to ensure all employees, volunteers, business associates, and students are subject to sanctions for any and all unauthorized use of protected health information. Sanctions will be appropriately and consistently enforced according to the guidelines set forth in this policy. Sanctions do not apply to disclosures made by whistle-blowers or employees who are victims of a crime.

**PROCEDURE:**

1. All complaints go to the Compliance Officer and/or the Privacy Officer.
2. All reported privacy breaches will be investigated by the Compliance Officer and the Director of Human Resources to determine validity.
3. When a privacy breach has been established, the Compliance Officer and the Director of Human Resources will refer the matter to the employee’s immediate supervisor and their respective Senior Management Team member.
4. The immediate supervisor and the Senior Management will evaluate the violation and determine the appropriate sanctions. They will notify the Corporate Compliance Officer of their decision.
5. The immediate supervisor will complete appropriate paperwork and forward to the Director of HR.
6. Sanctions will be determined by the following guidelines:
  - a. Accidental Violation: Members of the workforce determined to have unintentionally disclosed or used PHI inappropriately due to negligence, or misunderstanding are subject to the following sanctions:
    - i. Written warning and counseling by immediate supervisor

**DEPARTMENT:** Compliance

**POLICY TITLE:** CMP20 Sanctions for HIPAA Violations



- ii. Repeat of HIPAA training, administered by immediate supervisor or designee
- iii. Disciplinary action, up to and including termination, based on the seriousness and outcome of the breach, and whether this is the employee's first privacy violation.
- iv. Possible civil fines or penalties for negligently disclosing medical information under the California Medical Information Act
- b. Willful Violation: Members of the workforce determined to have knowingly and willfully obtained, used or disclosed Protected Health Information (PHI) indiscriminately outside of their job responsibilities, whether or not for profit or gain, are subject to the following sanctions:
  - i. Immediate termination without opportunity for rehire
  - ii. Possibility of investigation by The Office of Civil Rights (OCR)
  - iii. The OCR may choose to impose a civil monetary penalty, or notify the Department of Justice, and recommend criminal prosecution
  - iv. Possibility of civil fines or penalties under the California Medical Information Act

### **Breach and Termination of Business Associate Contracts**

1. It is the responsibility of every employee to report any knowledge of any matter of activity or practice on the part of a Business Associate that violated or breaches patient privacy. Any such observation should be reported to the Compliance Officer immediately.
2. The Compliance Officer will be responsible for working with Administration to notify the Business Associate of the breach and ensuring that responsible steps are taken to immediately cure the breach.
3. If steps to cure the breach are unsuccessful, Covered Entity will terminate the Business Associate Agreement for non-compliance.

### **Reporting Non-Compliance**

If termination is not possible, the problem will be reported to the Secretary of the Department of Health and Human Services.

**DEPARTMENT:** Compliance

**POLICY TITLE:** CMP20 Sanctions for  
HIPAA Violations



**DEFINITIONS:**

None

**REFERENCES:**

Heritage Provider Network Policies  
45 CFR §164.530(e)  
45 CFR § 164.502(j)

**APPENDICES:**

None

**DEPARTMENT:** Compliance

**POLICY TITLE:** CMP20 Sanctions for HIPAA Violations



**DOCUMENT REVISION LOG**

<b>Date</b>	<b>Document Modification (including deletions)</b>	<b>Page(s)</b>	<b>Location</b>
11/2019	Converted to AZPC template	All	All