SCOPE: PeaceHealth caregivers, affiliated physicians and other health care providers, their office staff, volunteers, vendors, students, contractors ("users").

PURPOSE: PeaceHealth is committed to protecting the confidentiality of patient and business information. This commitment is reflected in PeaceHealth's mission, standard of conduct, and in its policies and procedures. The following policy sets forth the actions PeaceHealth will take towards users when there is an allegation that a user has breached the confidentiality of PeaceHealth information.

POLICY: Maintaining the confidentiality of PeaceHealth information is an integral part of quality and compassionate care and therefore, a breach of confidentiality is subject to formal guidance as set forth in this policy. Confidential information includes patient and business information obtained or maintained by PeaceHealth. A breach of confidentiality for the purposes of this policy occurs when a user:

- **acquires, accesses, or reviews** patient or business information for any reason not related to the provision of care and treatment, payment, health care operations, or another authorized purpose;

- **discusses with, reveals, or discloses** to any individual(s) confidential information about PeaceHealth or about a patient for purposes not related to patient care or other authorized purpose; or,

- **violates the provisions** of PeaceHealth's Policies on Confidentiality, Security, and Privacy of PeaceHealth Information or any state/federal laws and regulations related to the security, privacy, and confidentiality of information.

Breaches of confidentiality may result in corrective action/performance improvement up to and including termination of employment, privileges, and/or access rights to PeaceHealth information. Reports will be made to applicable licensing boards and other regulatory agencies as required by applicable law and regulation. Violations of a criminal nature will be reported to the appropriate authorities.

PeaceHealth may be required to notify individuals who are the subject of any type of breach as described above including a description of the circumstances of the breach.

Criminal conviction for wrongful uses or disclosures: Users may be subject to criminal conviction by the federal government for unauthorized acquisition, access, use or disclosure of information obtained or maintained by PeaceHealth whether or not PeaceHealth has investigated a breach in accordance with this policy.

REQUIREMENTS:

Process for Investigation and Applicable Guidance
(Exception: Any portion of this policy that is inconsistent with any applicable collective bargaining agreement shall be governed by such collective bargaining agreement.)

1. **Initial Reporting – Use of the Chain of Command.** Persons who observe or are aware of a breach shall report the breach as soon as possible to any of the following:
   - Immediate supervisor, manager or director
   - Privacy Officer
   - IST Security Manager
   - Organizational Integrity (OI) Officer
   - Integrity Line
   - Electronic Incident Report

   Confidentiality is critical to our quality of care and therefore failure to report an alleged breach or reporting of an alleged breach in bad faith may result in corrective action/performance improvement.

2. **Investigation.** The Privacy Officer and/or HR breach team member or designee, shall investigate the alleged breach, in conjunction with the user's manager. The necessary and appropriate investigation, in accordance with the Notification Requirements for Breaches of Personal Information policy, e and may include interviewing the user believed to have committed the breach, interviewing additional individuals, and reviewing documentation. Verification of a breach could include patient, user, user's supervisor, witness interviews, and/or audits of the electronic systems.

3. **Process for Initiating Guidance.** The Community Breach Team will review the alleged breach and investigation findings complete the documentation for the risk of compromise, and identify a suggested guidance plan to recommend to HR or 3rd party management. The report will be tracked in the breach-tracking tool. This process may include a consultation with the System Legal Department as required.

4. **Notification of Affected Individuals.** PeaceHealth may be required to notify the individual whose information was accessed, used or disclosed. Refer to the Notification Requirements for Breaches of Personal Information policy.

5. **Documentation.** Information on the alleged breach and related written documentation shall be handled in a discreet manner. Pertinent information regarding alleged and confirmed breaches is to be recorded in the breach tracking tool maintained by the Privacy Officer. Guidance, including corrective action and appropriate related documentation shall be placed in the individual's applicable record. Individuals who dispute the action taken should refer to relevant policies, agreements, or other documents to determine the action they may take.

6. **Removal and Re-Application of Access.** As part of the disciplinary process a user's access may be removed when situations warrant such action. A user may reapply for access after one year by writing a letter of request and explanation to the community breach team. The community breach team will review the investigation details and evaluate the request. The

community breach team may consult with the system breach counterpart team or Legal, as needed. The user will be contacted, in writing, regarding the acceptance or rejection of their request.

DEFINITIONS:

The term "*corrective action/performance improvement*" includes counseling, education, verbal warning, written warning, final written warning, suspension, or termination as outlined by Human Resource policy.

REFERENCES:

Job Aids & Tools:

- **Issue Tracker**

Risk of Compromise Documentation:

- PH Breach Assessment Tool
- PH Breach Incident Assessment Tool
- PH Breach Assessment Process Algorithm

Policy Documents:

- OIC Breach Procedures
- Policy #SYS.169.7 PeaceHealth Application Audits
- Policy #SYS.38.17 Notification Requirements for Breaches of Personal Information
- Policy #SYS.38.3 Reporting of and Responding to Security Incidents
- Policy #SYS.38.34 Confidentiality, Security, and Privacy of PeaceHealth Information
- Policy #SYS.38.8 Accessing Confidential Information While Troubleshooting and/or Testing
- Policy #SYS.52.166 Corrective Action
- Procedure # SYS.38.77 Breach Team Procedures

HELP: For questions about this policy, or assistance with understanding your obligations under this policy, please contact your Privacy Officer.

End of Policy

The last page of this policy document contains approval, review and revision information only.

ORIGINAL VERSION:

Author:			
Responsible Party:	Carol Barnett; System Director of Organizational Integrity		
Reviewed By:			
Approved By:	John Hayward; CEO	**Date:**	11/11/2002
Replaces:			

PERIODIC REVIEW:

Reviewer:	SPOT	**Date:**	7/21/06
Reviewer:		**Date:**	
Reviewer:		**Date:**	

CAH ANNUAL REVIEW:

Reviewer/Facility:		**Date:**	
Reviewer/Facility:		**Date:**	
Reviewer/Facility:		**Date:**	

REVISIONS:

Version #:	**Responsible Party:**	Carol Barnett		
	Revised By:	Carol Barnett and Alice Becker		
	Reviewed By:	SPOT; System-wide Breach Team	**Date:**	
	Approved By:	SPOT	**Date:**	9/5/2013
	Reason/Summary of Changes:	Removed levels of breach and changed regional to community		
	Replaces:			
Version #:	**Responsible Party:**	Tonya Erickson; Technical Security Manager		
	Revised By:	Rayelene Dougherty; System Policy Coordinator		
	Reviewed By:		**Date:**	
	Approved By:	Not Required	**Date:**	1/16/2013
	Reason/Summary of Changes:	Changed HID to IST		
	Replaces:			
Version #:	**Responsible Party:**	Carol Barnett; System Director of Organizational Integrity		
	Revised By:	System-Wide Breach Team		
	Reviewed By:		**Date:**	
	Approved By:	SPOT	**Date:**	01/16/2012
	Approved By:	Alan Yordy; President and CMO	**Date:**	01/30/2012
	Reason/Summary of Changes:	Added language to clarify levels; removal of caregiver references.		
	Replaces:			

Version #:	**Responsible Party:**	Carol Barnett; System Director of Organizational Integrity		
	Revised By:	System-Wide Breach Team		
	Reviewed By:		**Date:**	
	Approved By:	SPOT	**Date:**	06/02/2011
	Approved By:	Alan Yordy; President and CMO	**Date:**	06/02/2011
	Reason/Summary of Changes:	Entire policy updated; added language to clarify levels and access re-application time frame.		
	Replaces:			

RETIRED:

Requested By:			
Approved By:		**Date:**	
Reason for Retirement:			