



健
計
劃
保

Chinese
Community
Health
Plan

CCHP

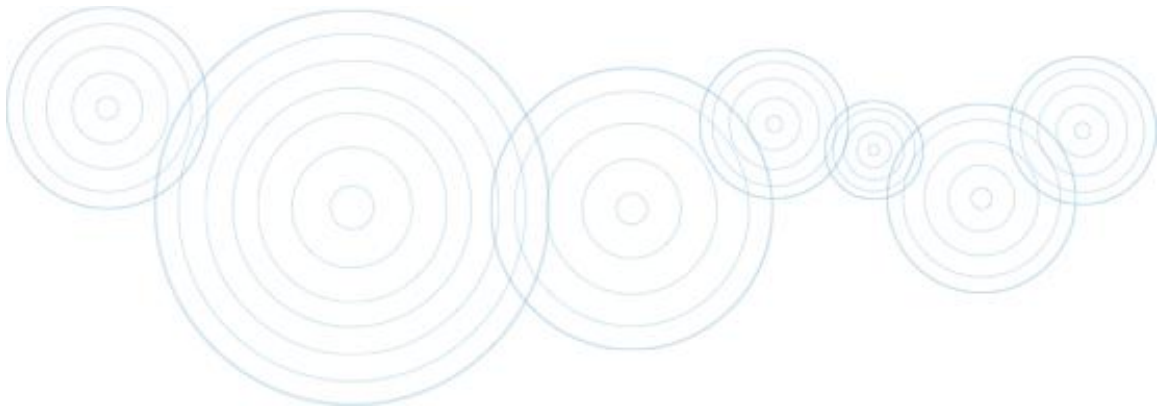


SECTION 17



HIPAA PROTECTED HEALTH INFORMATION

HIPAA Protected Health Information Policy	1
Computer Security Incident Report (CSIR) Form	4





Policy Number	13-2.20
Line of Business	Commercial and Medicare Advantage
Initial Date	5-27-2011
Revision Date(s)	
Approval	
Page(s)	8

TITLE: HIPAA Protected Health Information

PURPOSE:

To establish guidance regarding each provider’s responsibility related to identifiable Member information. This policy addresses an intentional or unintentional breach of Member confidentiality, including oral, written and electronic communication. This definition will safeguard Member privacy and help minimize exposure and/or liability to Members, providers, facilities and CCHP. Providers must comply with the federal Health Insurance Portability and Accountability Act (“HIPAA”) laws and regulations including, but not limited to the privacy and security of Members’ protected health information (“PHI”) as required by the Health Insurance Portability and Accountability Act (“HIPAA”), Standards for Privacy of Members’ Identifiable Health Information, 45 CFR Parts 160 and 164; the administrative, physical, and technical safeguards of the HIPAA Security Rule, as required by the Health Information Technology for Economic and Clinical Health Act (HITECH Act) as part of the American Recovery and Reinvestment Act of 2009; and any and all Federal regulations and interpretive guidelines promulgated there under.

POLICY:

1. Providers must make reasonable efforts to safeguard the privacy and security of Members’ PHI and are responsible for adhering to this policy by using only the minimum information necessary to perform his or her responsibilities, regardless of the extent of access provided or available.
2. Providers are allowed to release Member PHI to CCHP, without prior authorization from the Member, if the information is for treatment, payment or health care operations related to CCHP plans or programs.
3. Providers must notify CCHP, their Members; the Centers for Medicare and Medicaid (CMS); and the U.S. Department of Health & Human Services (DHHS) of any suspected or actual breach regarding the privacy and security of a Member’s PHI within prescribed timelines and through electronic submission formats.





DEFINITION:

“Protected Health Information” or “PHI” means any information, whether oral or recorded in any form or medium that relates to the past, present, or future physical or mental condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual; and that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual. PHI shall have the meaning given to such term under HIPAA and HIPAA regulations, as the same may be amended periodically.

PROCEDURE:

1. Only providers and their respective staff members with a legitimate “need to know” may access, use or disclose member information. This includes all activities related to treatment, payment and health care operations on behalf of CCHP. Each provider and their respective staff members may only access, use or disclose the minimum information necessary to perform his or her designated role regardless of the extent of access provided to him or her.
2. With respect to system access, member privacy will be supported through authorization, access, and audit controls and should be implemented for all systems that contain identifying member information. Within the permitted access, a member system user is only to access what they need to perform his or her job.
3. Each provider is responsible for attending ongoing education on member privacy and member rights as directed.
4. Each provider is responsible for compliance with these Protected Health Information policies and principles.
5. Permitted Uses and Disclosures
 - A. Except as otherwise required by law, Providers are allowed to release Member information, including PHI, without Member authorization, to CCHP for treatment, payment, or health care operations related to CCHP plans or programs.
 - B. Activities which are for purposes directly connected with the administration of services include, but are not limited to:
 - (1) Establishing eligibility and methods of reimbursement;
 - (2) Determining the amount of medical assistance;
 - (3) Arranging or providing services for Members;
 - (4) Conducting or assisting an investigation, prosecution, or civil or criminal proceeding related to the administration of CCHP plans or programs;
 - (5) Conducting or assisting in an audit related to the administration of CCHP plans or programs.





6. Reporting of Improper Disclosures

A. Providers are required to report unauthorized disclosures to:

- (1) CMS within one (1) hour during a work week from the time that the breach was identified. Please see Attachment B for electronic submission of the required electronic report format for submission to CMS which can also be accessed on the CCHP Website under the Provider tab.
- (2) The U.S. Department of Health & Human Services (DHHS) for breaches of unsecured PHI, sent electronically without unreasonable delay and in no case later than sixty (60) days from discovery of a breach affecting 500 or more individuals; and, electronic notice sent annually by March 1st for DHHS defined breaches that have occurred during the previous year that affected fewer than 500 individuals. Please see Attachment B for electronic submission of breaches affecting 500 or more individuals to DHHS which can also be accessed on the CCHP Website under the Provider tab. For annual reportable breaches affecting fewer than 500 individuals, access the DHHS Website:
<http://transparency.cit.nih.gov/breach/index.cfm>.
- (3) The CCHP Member(s) who's PHI has been breached in accordance with CMS and DHHS requirements.
- (4) The CCHP Corporate Compliance Officer within the regulatory timeline requirements of CMS and DHHS. Copies of the electronic submissions sent to CMS and/or DHHS may be sent to CCHP as notification of Member breaches.

Corporate Compliance Officer

Chinese Community Health Plan

445 Grant Ave., Ste. 700

San Francisco, CA 94108

Corporate Compliance Hotline: (415) 955.8810

Fax: (415) 955.8818

E-mail: cdobry@cchphmo.com

- (5) Providers must take prompt corrective action to mitigate and cure the cause(s) of the unauthorized disclosure.





CMS COMPUTER SECURITY INCIDENT REPORT (CSIR)

Date/Time: _____

Incident Tracking Number		
HHS (incident identification (ID) number provided by HHS CSIRC)	OPDIV (incident ID number provided by the Operating Division (OPDIV) reporting the incident)	US CERT (incident ID number provided by the United States Computer Emergency Readiness Team)

Reporting Individual Contact Information			
Name*			Email*
Office Number*	Cell Number	Dept/OPDIV*	UserID
Name(s) of Dept/OPDIV or individual notified of security incident:			
Dept/OPDIV	Name/Title	Date/Time Notified	

Impacted Location*	
Address	City/State/Zip

Impacted User Contact Information			
Name*			Email*
Office Number*	Cell Number	Dept/OPDIV*	UserID

Incident Category*	
<input type="checkbox"/> Lost/Stolen Asset (<i>Section A</i>)(Cat 0)	<input type="checkbox"/> Exercise/Network Defense Testing (<i>Section F</i>)
<input type="checkbox"/> PII Breach (<i>Section B mandatory</i>)	<input type="checkbox"/> Denial of Service (<i>Section G</i>) (Cat 2)
<input type="checkbox"/> Malicious Code (<i>Section C</i>) (Cat 3)	<input type="checkbox"/> Scans/Probes/Attempted Access (<i>Section G</i>) (Cat 5)
<input type="checkbox"/> Unauthorized Access (<i>Section D</i>) (Cat 1)	<input type="checkbox"/> Investigations (<i>Section G</i>) (Cat 6)
<input type="checkbox"/> Improper Usage (<i>Section E</i>) (Cat 4)	<input type="checkbox"/> Reportable Events (<i>Section H</i>) (Cat RE)





Type of Device Involved in Incident*

Devices			Operating System	
<input type="checkbox"/> Blackberry	<input type="checkbox"/> E-mail	<input type="checkbox"/> PDA	<input type="checkbox"/> Windows	
<input type="checkbox"/> Cell phone	<input type="checkbox"/> Hard Drive (External)	<input type="checkbox"/> Server	<input type="checkbox"/> Linux	
<input type="checkbox"/> Computer (Non-specific)	<input type="checkbox"/> Hard Drive (Internal)	<input type="checkbox"/> Tape/DLT/DASD	<input type="checkbox"/> Unix	
<input type="checkbox"/> Computer Files	<input type="checkbox"/> Laptop	<input type="checkbox"/> USB Thumb Drive	<input type="checkbox"/> Mac	
<input type="checkbox"/> Desktop Computer	<input type="checkbox"/> Paper Documents	<input type="checkbox"/> Other _____		
<input type="checkbox"/> Domain Controller	<input type="checkbox"/> CD/DVD			
Source IP/Network (Attacker)			Destination IP/Network (Victim)	
Source Computer Name (if known)			Destination Computer Name (if known)	
Anti-virus vendor			Anti-virus Signature Version Number	
Encryption			Encryption Type/Vendor	
<input type="checkbox"/> YES	<input type="checkbox"/> NO			

Section A: Lost/Stolen Asset

PII Involved? (if so, complete Section B)	Brief Description Include actions taken, asset brand/model, date and time, location of theft/damage and whether or not PII was exposed
<input type="checkbox"/> YES <input type="checkbox"/> NO	

Section B: PII Related Incident

Breach Category		
<input type="checkbox"/> Document Theft	<input type="checkbox"/> Document Lost in Transit	<input type="checkbox"/> Unauthorized Access
<input type="checkbox"/> Hardware/Media Theft	<input type="checkbox"/> Hardware/Media Lost in Transit	<input type="checkbox"/> Hacking or IT Incident
<input type="checkbox"/> Document Loss	<input type="checkbox"/> Improper Usage	<input type="checkbox"/> Document sent to Wrong Address
<input type="checkbox"/> Hardware/Media Loss	<input type="checkbox"/> Unintended Manual Disclosure	
	<input type="checkbox"/> Unintended Electronic Disclosure	





Number of PII Lost or Compromised
List Number below

Exact number of PII: _____ Otherwise check: Unknown

Brief Description:

Ensure to include the format of the PII (i.e. email, web, database, etc), population effected, lost/stolen, summary time stamp and the actions taken if any.

High-level Executive Summary

Detailed Incident Description

Section C: Malicious Code

Malware Type (Check One)

- Worm
- Virus
- Trojan
- Buffer Overflow

Denial of Service (DoS)
Other _____

Operating System?

- Windows
- Linux
- Unix
- Mac

Name of Malware if known





Action taken regarding Malware?			Prior to Event, was effected node properly patched?
<input type="checkbox"/> Quarantined	<input type="checkbox"/> Cleaned	<input type="checkbox"/> Left Alone	<input type="checkbox"/> Yes <input type="checkbox"/> No
Description of current actions taken (if any):			

Section D: Unauthorized Access

Describe Violation

Actions taken (if any)

Section E: Improper Usage/Policy Violation

Type of Violation					
(P2P) File Sharing	Instant Messenger	Inappropriate Web sites	Remote Access	Unapproved Software	Other (Describe)
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	

Describe Violation: (i.e. software name and version, URL address if applicable)

Describe Incident





Actions taken (if any)

Section F: Exercise/Network Defense Testing

Section G: Denial of Service, Scans/Probes/Attempted Access, & Investigations

Describe Violation
Actions taken (if any)

Section H: Reportable Events

Describe Violation
Actions taken (if any)
If Reportable Event Results in an Overpayment Provide Description

Testing Approval provided by	Contact Number	Testing Time Period
Brief Description: Include reason for testing and the networks and systems tested.		

