	POLICIES AND PROCEDURES
Policy #: 105-4012	**Lead Department:** Compliance
Title: Use and Disclosure of PHI, including Member Authorizations to Disclose	
Original Date: 05/01/2014	**Policy Hub Approval Date:**
Approved by: Jenifer Mandella, Compliance Officer	

Purpose:
The purpose of this policy is to provide an overview of when Protected Health Information (PHI) may and must be disclosed with or without a Member's or Member's Personal Representative's authorization. Additionally, the purpose of this policy is to describe the procedures for using or disclosing a Member's PHI with a valid authorization, in accordance with state and federal laws.

Policy:
It is Central California Alliance for Health's (the Alliance's) policy to protect the privacy of Members and to use and/or disclose PHI consistent with state and federal laws. Requests for access to PHI are reviewed to determine a need for an authorization from the Member or their Personal Representative. If the use or disclosure is either required or permissible without an authorization, the Alliance will verify the requestor's identity and approved authority, to ensure that all efforts are made to minimize any impermissible access, use, disclosure, modification, or destruction of PHI. When PHI may be used and/or disclosed only with authorization from the Member, the Alliance will obtain the Member's or Member's Personal Representative's authorization prior to disclosing PHI.

Definitions:
Refer to *HIPAA-HITECH Privacy and Security Glossary*.

Procedures:
Following is a description of when PHI may or must be released without the Member or Member's Personal Representative's authorization, and when an authorization is required to release PHI. Note that the Alliance maintains detailed policies describing each of these required and permitted disclosers. Alliance staff are to refer to those supplemental policies in determining whether the release of PHI is appropriate.

1. When Authorization is Not Required[i]
   a. Required Disclosures:
      i. To Members or their Personal Representatives.[ii]
      ii. To health oversight agencies for the purposes of demonstrating the Alliance's compliance with the Privacy Rule. [iii] [iv]
      iii. Any other disclosures that are required by law.[v]
   b. Permitted Disclosures:
      i. Uses and Disclosures for Treatment, Payment, and Health Care Operations, including disclosures to Business Associates, pursuant to a Business Associate Agreement.[vi]

ii. Disclosures to law enforcement or government officials in response to a legal process, including court order, warrant, subpoena, or administrative request.
iii. Disclosures of PHI of deceased Members to certain recipients.
iv. Certain promotional communications to the Member, such as periodic reminders about coverage, services, or benefits; or, general health information materials.
v. In a Limited Data Set for the purposes of research or public health.

2. Disclosures Requiring an Opportunity to Agree or Object. The following types of disclosures require that the Member or Member's Personal Representative be provided with an opportunity to agree or object to the disclosure of PHI[vii]:
   a. Disclosures to family, caregivers, family, and friends for the purposes of coordinating treatment.
   b. Disclosures for disaster relief.
   c. Disclosures in response to a subpoena or other legal or administrative process.

3. When Authorization is Required. All other disclosures of PHI that are not considered required or permissible, including but not limited to, disclosures of substance abuse information, HIV/AIDS information, psychotherapy notes and/or information about mental health received in an institutional setting, or through a state or county sponsored program, requires a valid written authorization from the Member.[viii]
   a. If an authorization is required, only the Member, the Member's Personal Representative, or an executor or conservator on behalf of the Member may authorize the use or disclosure of the Member's PHI. A written authorization may only be signed by a representative on behalf of the member after verification of the identity and authority of the requestor by providing acceptable credentials or documentation to the Alliance. The authority of the representative must be indicated on the authorization form.
   b. If the Alliance initiates the request for authorization, the Alliance will maintain the signed authorizations on file a minimum of 6 years. The member may request a copy of their signed authorization at any time.[ixx]

4. Minimum Necessary. Only the information specified in an authorization may be used or disclosed and the terms of the authorization must be followed. If the authorization appears vague or overly broad, the Alliance's Privacy Officer or designee will review the authorization and may contact the Member, as

appropriate, to determine the appropriate amount of information to be used or disclosed.

5. Valid Authorizations. Authorizations must be written in plain language and include the core elements of a valid authorization:[xi] [xii]
   - A specific and meaningful description of the information to be disclosed.
   - The name of the person authorized to make the request.
   - The name or specific identification of the person(s) to whom the Alliance can make the disclosure.
   - A description of each purpose of the request use or disclosure. "At the request of the individual" is sufficient.
   - An expiration date or expiration event. If the disclosure is for research, "end of research study" or "none" is sufficient.
   - Signature of the Member or Member's Personal Representative and date. Must include a description of any authorized representatives.

   In addition, the following information is required:
   - The Member's right to revoke the authorization and any exceptions.
   - The member's refusal to sign the authorization will not affect the member's enrollment in the Plan or impact the member's eligibility to receive benefits.

6. Defective Authorizations.[xiii] An authorization cannot be accepted if it has any of the following defects:
   a. The expiration date has passed, or the authorization specifies a particular expiration event that is known to have occurred.
   b. The authorization does not include all required core elements described in Procedure 5 – Valid Authorizations.
   c. The authorization is known to have been revoked, even if the Alliance has not yet received a copy of the written revocation.
   d. The authorization has been combined with other documents or types of permissions, unless one of the exceptions in Procedure 7 – Compound Authorizations has been met.
   e. Any material information in the authorization is known by the Alliance to be false.

7. Compound Authorizations.[xiv] An authorization for use or disclosure of PHI may not be combined with any other document to create a compound authorization, except as follows:
   i. An authorization for the use or disclosure of PHI for a research study may be combined with any other type of written permission for the same or another research study.
   ii. An authorization for a use or disclosure of psychotherapy notes may only be combined with another authorization for a use or disclosure of psychotherapy notes;

8. Validating Authorizations. Alliance staff will validate authorizations to ensure all required elements are included prior to disclosing PHI. Validated authorizations will be forwarded to Compliance for retention.

9. Revocation. The Member or the Member's Personal Representative may revoke an authorization at any time. The revocation must be in writing and will be signed by the Member's representative. The revocation does not affect any uses or disclosures made by the Alliance prior to the revocation.[xv]

10. Revoked or Expired Authorization. Upon revocation or expiration of an authorization, the authorization form will be clearly marked to show that it is no longer valid. When a revocation is received, Compliance staff will scan the written revocation and retain a copy of the revocation. Compliance staff will ensure that revocations are forwarded to applicable business associates or subagents.

11. No Denial of Treatment or Enrollment in Plan or Eligibility for Benefits. Treatment, enrollment in a Customer plan, or eligibility for benefits will not be denied solely because a Member refuses to sign an authorization. Potential exceptions include[xvi]:
    - Research-related treatment.
    - Physicals and screenings paid for by employers or insurers.

References:

Alliance Policies:

105-4008 – Uses and Disclosures of Limited Data Sets
105-4009 – Minimum Necessary Use and Disclosure

105-4018 - Personal Representative
105-4020 – Disclosures to Law Enforcement and Government Officials
105-4021 – Uses and Disclosures about Decedents
105-4025 – Uses and Disclosures for Health Oversight Activities
105-4023 – Disclosures for Public Health Activities
200-1003 – Member Designation of Personal Representatives

Impacted Departments:
Care Management
Member Services

Regulatory:
45 CFR §164.502(a)
45 CFR § 164.508(a)-(c)
45 CFR §164.512(d)

Legislative:
CA Civil Code 56.10
CA Civil Code 56.104

Contractual:
Medi-Cal Contract Exhibit G, Attachment A.II.C
Medi-Cal Contract Exhibit A, Section 18, Provision 17 & 18

MMCD Policy Letter:

NCQA:

Supersedes:
Policy 100-2007 – Protected Health Information Authorization/Revocation
Policy 105-4006 – Required and Permissible Uses and Disclosures

Other References:

Attachments:

Lines of Business This Policy Applies To	**LOB Effective Dates**
☒ Medi-Cal	(01/01/1996 – present)
☒ Alliance Care IHSS	(07/01/2005 – present)

Revision History:

Reviewed Date	**Revised Date**	**Changes Made By**	**Approved By**
11/06/2015	11/06/2015	Nicole Krupp, Compliance	HIPAA Project Workgroup

		Specialist	
07/26/2016	07/26/2016	Nicole Krupp, Compliance Specialist	Jenifer Mandella, Compliance Director
10/05/2017	10/05/2017	Paige Harris, Compliance Specialist	Jenifer Mandella, Compliance Officer
08/07/2018	08/17/2018	Paige Harris, Compliance Specialist	Jenifer Mandella, Compliance Officer
09/06/2019	09/06/2019	Paige Harris, Compliance Specialist	Jenifer Mandella, Compliance Officer

[i] 45 CFR §164.502(a)(1)
[ii] 45 CFR §164.502(a)(2)(i)
[iii] 45 CFR §164.502(a)(2)(ii)
[iv] 45 CFR §164.512(d)
[v] CA Civil Code 56.10(b)
[vi] 45 CFR §164.502(a)(1)(ii)
[vii] 45 CFR §164.502(a)(1)(v)
[viii] 45 CFR 164.508(a)
[ix] 45 CFR § 164.508(b)(6)
[x] 45 CFR § 164.508(c)(4)
[xi] 45 CFR § 164.508(b)(1)
[xii] 45 CFR § 164.508(c)(1) – (c)(3)
[xiii] 45 CFR § 164.508(b)(2)
[xiv] 45 CFR § 164.508(b)(3)
[xv] 45 CFR § 164.508(b)(5)
[xvi] 45 CFR § 164.508(b)(4)

Central California Alliance for Health
HIPAA-HITECH Privacy and Security Glossary

Audit Log- a security relevant chronological record, set of records, and/or destination and source of records that provide documentary evidence of the sequence of activities that have affected at any time a specific operation, procedure, or event.

Breach- the acquisition, access, use or disclosure of protected health information which compromises the security or privacy of the protected health information. At the Alliance, a breach can only be determined by the HIPAA Officers or Compliance Officer.

Business Associate (BA) - a person or organization that performs a function or activity involving the use or disclosure of protected health information, on behalf of the covered entity. A person or organization who only assists in the performance of the function or activity is also a business associate. This includes a person or organization that receives PHI from the covered entity, and one who obtains PHI for the covered entity.

Caregiver – a Member's family, other relatives, close personal friends or other persons identified by the Member as involved in the Member's care of payment of care.

Covered entity (CE) - a health care provider that electronically transmits health information for any of the standardized transactions, a health plan, or a health care clearinghouse.

Data Backup- the result of copying or archiving files and folders for the purpose of being able to restore them in case of data loss.

Data at Rest- refers to data stored in persistent storage (disk, tape).

De-identified Health Information - health information from which individual identifiers have been removed, so that it cannot be used to identify an individual. De-identified health information is not protected by HIPAA.

Disclosures- the release, transfer, provision of, access to, or divulging in any other manner of protected health information (PHI) outside the covered entity holding the information.

Electronic Protected Health Information (EPHI)- all individually identifiable health information that is created, maintained or transmitted electronically.

Emancipated Minor: a minor who is not legally an adult but is entitled to be treated as one due to a court order, marriage, military service, etc. Once a minor becomes emancipated, his or her parents no longer have custody and minors are able to make healthcare decisions without parental consent.

Encryption- the process of protecting data by making it unreadable to unauthorized third parties.

Event - the acquisition, access, use or disclosure of protected health information which has the possibility of compromising the security or privacy of the protected health information.

Health care operations- certain administrative, financial, legal, and quality improvement activities of a covered entity that are necessary to run its business and to support the core functions of treatment and payment.

HIPAA- Health Insurance Portability and Accountability Act of 1996 A Federal law that allows persons to qualify immediately for comparable health insurance coverage when they change their employment relationships. Title II, Subtitle F, of HIPAA gives the Department of Health and Human Services the authority to mandate the use of standards for the electronic exchange of health care data; to specify what medical and administrative code sets should be used within those standards; to require the use of national identification systems for health care patients, providers, payers and employers; and to specify the types of measures required to protect the security and privacy of personally identifiable health care information.

Incident- the acquisition, theft, access, use or disclosure of protected health information which has the high probability of or has compromised the security or privacy of the protected health information.

Law Enforcement Official - an officer or employee of any governmental agency who is empowered by law to investigate or prosecute violations of law.

Limited Data Set- health information that excludes specified direct identifiers of the Member or of relatives, employers, or household members of the Member

Media Access Control (MAC)- a unique identifier assigned to network interfaces for communications on the physical network segment.

Member - an individual enrolled in a Central California Alliance for Health plan.

Minimum Necessary – a standard that requires covered entities to evaluate their practices and enhance safeguards as needed to limit unnecessary or inappropriate access to and disclosure of Protected Health Information (PHI).

Minor – an individual who is under 18 years of age. Per CA state laws, minors are able to make their own healthcare decisions without parental/guardian consent dependent on the services and their age.

- At **any age** a minor may consent to medical care related to pregnancy, contraception, abortion, sexual assault services, rape services, emergency medical services, and skeletal x-ray to diagnose child abuse or neglect.

- Minors **12 years of age or older** may consent to the above medical care as well as medical care related to infection/contagious communicable diseases, sexually transmitted diseases, AIS/HIV testing and treatment, outpatient mental health services/shelter services, and drug/alcohol abuse treatment.
- Minors **15 years of age or older** may consent to the above medical care as well as medical care related to general medical care (14 years or older if the minor is emancipated).

Need to Know – minimum information staff can access based on job duties and role.

Notice of Privacy Practice (NPP) - a notice that a covered entity is required to make available to patients or enrollees describing how the entity uses and disclosures of protected health information, and the individual's rights with respect to protected health information.

Payment - encompasses the various activities of health care providers to obtain payment or be reimbursed for their services and of a health plan to obtain premiums, to fulfill their coverage responsibilities and provide benefits under the plan, and to obtain or provide reimbursement for the provision of health care.

Personal Representative- a person with legal authority to make health care decisions on behalf of the Member.

Pretty Good Privacy (PGP)- program used to encrypt and decrypt email over the internet.

Privacy Officer- the official appointed by a covered entity to be responsible for developing and implementing policies and procedures for complying with the health information privacy requirements of HIPAA.

Protected Health Information (PHI) - individually identifiable health information held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper or oral.

Remote Access- ability to get access to a computer or a network from a remote distance.

Role-Based Access – limits staff access to PHI dependent on job duties and roles.

Secure/Multipurpose Internet Mail Extensions (S/MIME)- a standard for public key encryption and signing of MIME data.

Security Management- the identification of an organization’s assets (including information assets), followed by the development, documentation, and implementation of policies and procedures for protecting these assets.

Security Officer- the official appointed by the covered entity to oversee security obligations under state and federal privacy laws.

Secure Socket Layer (SSL) Certificates- certificates that verify the authenticity of websites to browsers and ensure that data is encrypted over a secure network connection.

Simple Mail Transfer Protocol (SMTP)- an Internet standard for e-mail transmission.

Treatment- the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.

Virtual Private Network (VPN)- a network that uses a public telecommunication infrastructure, such as the internet, to provide remote offices or individual users with secure access to their organization.