

HIPAA PRIVACY & SECURITY PLAN

March 2012

TABLE OF CONTENTS

HIPAA Privacy & Security Plan

INTRODUCTION	1
SECTION 1: RESPONSIBILITIES OF COVERED ENTITY	1
Privacy Officer	
Incident Response Team	
Workforce Training	
Safeguards	
Privacy Notice	
Complaints	
Sanctions for Violations of Privacy Policy	
Mitigation of Inadvertent Disclosures of PHI	3
No Intimidating or Retaliatory Acts/No Waiver of HIPAA	4
Plan Document	4
Documentation	4
Electronic Health Records	5
Access Authorization	5
SECTION 2 – USE AND DISCLOSURE OF PHI	
Use and Disclosure Defined	
Access to PHI is Limited to Certain Employees	
Disclosures of PHI Pursuant to an Authorization	
Permissive Disclosures of PHI	
Complying with the "Minimum-Necessary" Standard	
Disclosures of PHI to Business Associates	
Disclosures of De-Identified Information	
Disclosures to Family, Friends or Others-Participant Location	
Removing PHI from Company Premises	
Faxing PHI	12
SECTION 3 – PARTICIPANT INDIVIDUAL RIGHTS	13
Access to PHI and Requests for Amendment	
Accounting	
Requests for Alternative Communication	
Requests for Restrictions on Uses and Disclosures of PHI	
When a Participant Requests a Copy of his/her Record	
Participants Request for Copy of Clinic Notes or Labs	
Acceptable Methods of Verification of Identification	
When the Requestor is the Participants Legally Authorized Representative	
Other Methods	
SECTION 4 – PHI BREACH REPORTING	17
Breach Notification Requirements	
Complaint/Concerns Reporting	
	10 10

ATTACHMENTS

- Summary Guidelines for Safeguarding the Privacy of Health Information
- Summary Notice of Privacy Practices
- Acknowledgment of Receipt of Summary Notice of Privacy Practices
- Authorization for Release and/or Disclosure of Health Information Form
- Request for Alternative Means of Communication of Protected Health Information Form
- Request for Accessing/Inspecting/Copying Health Information Form

- Request for Amendment of Health Information Form
- Request for Restrictions on Use and Disclosure of Health Information Form
- Accounting of Non-Authorized Use or Disclosure Request Form
- Business Associate Agreement Template
- Axis Fax Form
- Incident Report
- Complaint Form
- Federal & State Privacy Laws

HIPAA Privacy & Security Plan

Introduction

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its implementing regulations restrict Axis Community Health ("Axis", "Company") abilities to use and disclose protected health information (PHI).

Protected Health Information. Protected health information means information that is created or received by the Company and relates to the past, present, or future physical or mental health condition of a Patient/Client ("Participant"); the provision of health care to a participant; or the past, present, or future payment for the provision of health care to a participant; and that identifies the participant or for which there is a reasonable basis to believe the information can be used to identify the participant. Protected health information includes information of persons living or deceased.

Some examples of PHI are:

- Participant's medical record number
- Participant's demographic information (e.g. address, telephone number)
- Information doctors, nurses and other health care providers put in a participant's medical record
- Images of the participant
- Conversations a provider has about a participant's care or treatment with nurses and others
- Information about a participant in a provider's computer system or a health insurer's computer system
- Billing information about a participant at a clinic
- Any health information that can lead to the identity of an individual or the contents of the information can be used to make a reasonable assumption as to the identity of the individual

It is the Company's policy to comply fully with HIPAA's requirements. To that end, all staff members who have access to PHI must comply with this HIPAA Privacy and Security Plan. For purposes of this plan and the Company's use and disclosure procedures, the workforce includes individuals who would be considered part of the workforce under HIPAA such as employees, volunteers, interns, board members and other persons whose work performance is under the direct control of Axis, whether or not they are paid by Axis. The term "employee" or "staff member" includes all of these types of workers.

No third party rights (including but not limited to rights of participants, beneficiaries, covered dependents, or business associates) are intended to be created by this Plan. Axis reserves the right to amend or change this Plan at any time (and even retroactively) without notice.

All staff members must comply with all applicable HIPAA privacy and information security policies. If after an investigation you are found to have violated the organization's HIPAA privacy and information security policies then you will be subject to disciplinary action up to termination or legal ramifications if the infraction requires it.

SECTION 1: Responsibilities as Covered Entity

I. Privacy Officer

The Human Resources Director will be the HIPAA Privacy Officer for Axis Community Health. The Privacy Officer will be responsible for the development and implementation of policies and procedures relating to privacy, including but not limited to this Privacy Policy and the Company's use and disclosure procedures. The Privacy Officer will also serve as the contact person for participants who have questions, concerns, or complaints about the privacy of their PHI. The Privacy Officer can be reached at (925) 201-6038.

II. Incident Response Team

The Incident Response Team is comprised of the CIO, COO, Site Managers and additional members deemed appropriate on an ad hoc basis in the reasonable judgment of the Privacy Officer. In the event of a security incident results in a wrongful disclosure of PHI, the Privacy Officer, in conjunction with the Incident Response Team will take appropriate actions to prevent further inappropriate disclosures. In addition, Human Resources and Legal may be consulted as part of the review team to assist in the review and investigation of privacy incidents when required. If the Privacy Officer and Incident Response Team have not resolved the incident, the Privacy Officer shall involve anyone determined to be necessary to assist in the resolution of the incident. If participants need to be notified of any lost/stolen PHI, the Privacy Officer will send PHI Theft/Loss Disclosure Letters to all possible affected individuals.

III. Workforce Training

It is the Company's policy to train all members of its workforce who have access to PHI on its privacy policies and procedures. All staff members receive HIPAA training. Whenever a privacy incident has occurred, the Privacy Officer in collaboration with management will evaluate the occurrence to determine whether additional staff training is in order. Depending upon the situation, the Privacy Officer may determine that all staff should receive training that is specific to the privacy incident. The Privacy Officer will review any privacy training developed as part of a privacy incident resolution to ensure the materials adequately address the circumstances regarding the privacy incident and reinforce the Company's privacy policies and procedures.

IV. Safeguards

The Company has established technical and physical safeguards to prevent PHI from intentionally or unintentionally being used or disclosed in violation of HIPAA's requirements. Technical safeguards include limiting access to information by creating computer firewalls. Physical safeguards include locking doors or filing cabinets and periodically changing door access codes. Additionally all staff members can only access PHI by using their own login information.

Firewalls ensure that only authorized employees will have access to PHI, that they will have access to only the minimum amount of PHI necessary for their job functions, and that they will not further use or disclose PHI in violation of HIPAA's privacy rules.

Data Storage / Backup / Remote Access

Currently all data in the local data center is backed up using industry standards with off site storage of media. Axis currently utilizes technology that allows the IT team to quickly remove, disable and start staff member access to PHI.

V. Privacy Notice

The Privacy Officer is responsible for developing and maintaining a notice of the Company's privacy practices that describes:

- the uses and disclosures of PHI that may be made by the Company;
- the individual's rights; and
- the Company's legal duties with respect to the PHI.

The privacy notice will inform participants that the Company will have access to PHI. The privacy notice will also provide a description of the Company's complaint procedures, the name and telephone number of the contact person for further information, and the date of the notice.

The notice of privacy practices will be individually delivered to all participants:

- on an ongoing basis, at the time of an individual's enrollment into a Company program or at the time of treatment and consent; and
- within 60 days after a material change to the notice.

The Company will also provide notice of availability of the privacy notice at least once every three years.

VI. Complaints

The Privacy Officer will be the Company's contact person for receiving complaints. The Privacy Officer is responsible for creating a process for individuals to lodge complaints about the Company's privacy procedures and for creating a system for handling such complaints. A copy of the complaint form shall be provided to any participant upon request.

VII. Sanctions for Violations of Privacy Policy

Sanctions for using or disclosing PHI in violation of this HIPAA Privacy Plan will be imposed in accordance up to and including termination.

VIII. Mitigation of Inadvertent Disclosures of Protected Health Information

Axis shall mitigate, to the extent possible, any harmful effects that become known to it because of a use or disclosure of an Participant's PHI in violation of the policies and procedures set forth in this Plan. As a result, if an employee becomes aware of a disclosure of protected health information, either by a staff member of the Company or an outside consultant/contractor that is not in compliance with this Policy, immediately contact the Privacy Officer so that the appropriate steps to mitigate the harm to the participant can be taken.

IX. No Intimidating or Retaliatory Acts; No Waiver of HIPAA Privacy

No employee may intimidate, threaten, coerce, discriminate against, or take other retaliatory action against individuals for exercising their rights, filing a complaint, participating in an investigation, or opposing any improper practice under HIPAA.

No individual shall be required to waive his or her privacy rights under HIPAA as a condition of treatment, payment, enrollment or eligibility.

X. Plan Document

The Plan document includes provisions to describe the permitted and required uses and disclosures of PHI by Axis. Specifically, the Plan document requires Axis to:

- not use or further disclose PHI other than as permitted by the Plan documents or as required by law;
- ensure that any agents or subcontractors to whom it provides PHI received from the Company agree to the same restrictions and conditions that apply to Axis;
- report to the Privacy Officer any use or disclosure of the information that is inconsistent with the permitted uses or disclosures;
- make PHI available to Participants, consider their amendments and, upon request, provide them with an accounting of PHI disclosures;
- make the Company's internal practices and records relating to the use and disclosure of PHI received by the Company available to the Department of Health and Human Services (DHHS) upon request; and

XI. Documentation

The Company's privacy policies and procedures shall be documented and maintained for at least six years. Policies and procedures must be changed as necessary or appropriate to comply with changes in the law, standards, requirements and implementation specifications (including changes and modifications in regulations). Any changes to policies or procedures must be promptly documented.

If a change in law impacts the privacy notice, the privacy policy must promptly be revised and made available. Such change is effective only with respect to PHI created or received after the effective date of the notice.

Axis shall document certain events and actions (including authorizations, requests for information, sanctions, and complaints) relating to an individual's privacy rights.

The documentation of any policies and procedures, actions, activities and designations may be maintained in either written or electronic form.

Incident Report

The Company has developed an Incident Report form. This form is used to document reports of privacy breaches that have been referred to the Privacy Officer from staff members who have reviewed or received the suspected incident.

After receiving the Incident Report form from staff members, the Privacy Officer classifies the incident and its severity and analyzes the situation. Documentation shall be retained by the Company for a minimum of six years from the date of the reported incident.

If the Privacy Officer is able to resolve the incident, the Privacy Officer shall also document the actions taken to resolve the issue in the Incident Report form.

XII. Electronic Health Records

Just like paper records, Electronic Health Records must comply with HIPAA, and other state and federal laws. Unlike paper records, electronic health records can be encrypted - using technology that makes them unreadable to anyone other than an authorized user - and security access parameters are set so that only authorized individuals can view them. Further, EHRs offer the added security of an electronic tracking system that provides an accounting history of when records have been accessed and who accessed them.

XIII. Access Authorization

Axis will grant access to PHI based on their job functions and responsibilities.

The Privacy Officer in collaboration with IT and senior management is responsible for the determination of which individuals require access to PHI and what level of access they require through discussions with the individual's manager and or department head.

The IT department will keep a record of authorized users and the rights that they have been granted with respect to PHI. IT keeps a comprehensive matrix of how and to who rights are granted. A summary of user rights can be found in the table below.

Job Title	Department	User rights
Patient Services	Call Center	Appointment Scheduling
	Referrals	Override Schedule - with RN approval
	Eligibility	View / Modify Patient Information
		Daily Appointment Reports
Front Desk / Medical Assistance	Clinic	Appointment Scheduling
Managers / Directors	BH Department	View / Modify Patient Information
		Daily appointment Reports
		Batch - Cash Management
		Transaction Entry
		Check-in -Create fee
		tickets

Job Title	Department	User rights
Medical Records Clerk	Medical Records	View Patient Information
		Run Chart Pull reports (daily appointments)
		View Schedule
Medication Refill	Medical Records	Appointment Scheduling
		View Patient Information
		Run Chart Pull reports (daily appointments)
RN Nurse Managers	Clinic	View Schedule
		Appointment Scheduling
		Override Schedule
		View / Modify Patient Information
		Daily Appointment Reports
IT - Department	IT Department	Schedule template -add/ modify
Department	Tr Department	Full System Administrative
Application Analyst		rights
Project Support		Full File Maintenance Level rights
		All operational functions in
Clinical Applications Manager HIT Coordinator		EPM
Behavioral Health Counselors	Behavior Health	appointment Scheduling
Interns	Denavior ricaltii	View / Modify patient information
mems		Daily Appointment Reports
Senior Staff	Admin	View/ Modify patient information
	Finance	Full report access
		Appointment Scheduling
		Cash Management / Transaction Entry and
		Modifications
Billing Clerk	Billing Department	Charge Entry
Billing Manager		Claim Entry
		Process Claim
		Financial Reports
		Payer Information / edit/
		modify

SECTION 2: Use and Disclosure of PHI

I. Use and Disclosure Defined

The Company will use and disclose PHI only as permitted under HIPAA. The terms "use" and "disclosure" are defined as follows:

- *Use.* The sharing, employment, application, utilization, examination, or analysis of individually identifiable health information by any person working for or within the Company, or by a Business Associate of the Company.
- *Disclosure*. For information that is protected health information, disclosure means any release, transfer, provision of access to, or divulging in any other manner of individually identifiable health information to persons not employed by or working within Axis with a business need to know PHI.

II. Access to PHI Is Limited to Certain Employees

All staff who performs Participant functions directly on behalf of the Company or on behalf of group health plans will have access to PHI as determined by their department and job description and as granted by IT.

These employees with access may use and disclose PHI as required under HIPAA but the PHI disclosed must be limited to the minimum amount necessary to perform the job function. Employees with access may not disclose PHI unless an approved compliant authorization is in place or the disclosure otherwise is in compliance with this Plan and the use and disclosure procedures of HIPAA.

Staff members may not access either through our information systems or the participant's medical record the medical and/or demographic information for themselves, family members, friends, staff members or other individuals for personal or other non-work related purposes, even if written or oral participant authorization has been given. If the staff member is a Participant in Axis's plans, the staff member must go through their Provider in order to request their own PHI.

In the very rare circumstance when a staff member's job requires him/her to access and/or copy the medical information of a family member, a staff member, or other personally known individual, then he/she should immediately report the situation to his/her manager who will determine whether to assign a different staff member to complete the task involving the specific Participant.

Your access to your own PHI must be based on the same procedures available to other participants not based on your job-related access to our information systems. For example, if you are waiting for a lab result or want to view a clinic note or operative report, you must either contact your physician for the information or make a written request to the Privacy Officer. You cannot access your own information; you must go through all the appropriate channels as any Participant would have to.

III. Disclosures of PHI Pursuant to an Authorization

PHI may be disclosed for any purpose if an authorization that satisfies all of HIPAA's requirements for a valid authorization is provided by the participant. All uses and disclosures made pursuant to a signed authorization must be consistent with the terms and conditions of the authorization.

IV. Permissive Disclosures of PHI: for Legal and Public Policy Purposes

PHI may be disclosed in the following situations without a participant's authorization, when specific requirements are satisfied. The Company's use and disclosure procedures describe specific requirements that must be met before these types of disclosures may be made. Permitted are disclosures:

- about victims-of abuse, neglect or domestic violence;
- for judicial and administrative proceedings;
- for law enforcement purposes;
- for public health activities;
- for health oversight activities;
- about decedents;
- for cadaver organ, eye or tissue donation purposes;
- for certain limited research purposes;
- to avert a serious threat to health or safety;
- for specialized government functions; and
- that relate to workers' compensation programs.

V. Complying With the "Minimum-Necessary" Standard

HIPAA requires that when PHI is used or disclosed, the amount disclosed generally must be limited to the "minimum necessary" to accomplish the purpose of the use or disclosure.

The "minimum-necessary" standard does not apply to any of the following:

- uses or disclosures made to the individual;
- uses or disclosures made pursuant to a valid authorization;
- disclosures made to the Department of Labor;
- uses or disclosures required by law; and
- uses or disclosures required to comply with HIPAA.

Minimum Necessary When Disclosing PHI. For making disclosures of PHI to any business associate or providers, or internal/external auditing purposes, only the minimum necessary amount of information will be disclosed.

All other disclosures must be reviewed on an individual basis with the Privacy Officer to ensure that the amount of information disclosed is the minimum necessary to accomplish the purpose of the disclosure.

Minimum Necessary When Requesting PHI. For making requests for disclosure of PHI from business associates, providers or participants for purposes of claims payment/adjudication or internal/external auditing purposes, only the minimum necessary amount of information will be requested.

All other requests must be reviewed on an individual basis with the Privacy Officer to ensure that the amount of information requested is the minimum necessary to accomplish the purpose of the disclosure.

VI. Disclosures of PHI to Business Associates

With the approval of the Privacy Officer and in compliance with HIPAA, employees may disclose PHI to the Company's business associates and allow the Company's business associates to create or receive PHI on its behalf. However, prior to doing so, the Company must first obtain assurances from the business associate that it will appropriately safeguard the information. Before sharing PHI with outside consultants or contractors who meet the definition of a "business associate," employees must contact the Privacy Officer and verify that a business associate contract is in place.

Business Associate is an entity that:

- performs or assists in performing a Company function or activity involving the use and disclosure of protected health information (including claims processing or administration, data analysis, underwriting, etc.); or
- provides legal, accounting, actuarial, consulting, data aggregation, management, accreditation, or financial services, where the performance of such services involves giving the service provider access to PHI.

Examples of Business Associates are:

- > A third party administrator that assists the Company with claims processing.
- > A CPA firm whose accounting services to a health care provider involves access to protected health information.
- > An attorney whose legal services involve access to protected health information.
- A consultant that performs utilization reviews for the Company.
- A health care clearinghouse that translates a claim from a non-standard format into a standard transaction on behalf of the Company and forwards the processed transaction to a payer.
- > An independent medical transcriptionist that provides transcription services for the Company.
- > A pharmacy benefits manager that manages a health plan's pharmacist network.

VII. Disclosures of De-Identified Information

The Company may freely use and disclose de-identified information. De-identified information is health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual. There are two ways a covered entity can determine that information is de-identified: either by professional statistical analysis, or by removing 18 specific identifiers.

18 specific elements listed below - relating to the participant, employee, relatives, or employer - must be removed, and you must ascertain there is no other available information that could be used alone or in combination to identify an individual.

- 1. Names
- 2. Geographic subdivisions smaller than a state
- 3. All elements of dates (except year) related to an individual including dates of admission, discharge, birth, death and for persons >89 y.o., the year of birth cannot be used.
- 4. Telephone numbers
- 5. FAX numbers
- 6. Electronic mail addresses
- 7. Social Security Number
- 8. Medical Record numbers
- 9. Health plan beneficiary numbers
- 10. Account numbers
- 11. Certificate/license numbers
- 12. Vehicle identifiers and serial numbers including license plates
- 13. Device identifiers and serial numbers
- 14. Web URLs
- 15. Internet protocol addresses
- 16. Biometric identifiers, including finger and voice prints
- 17. Full face photos, and comparable images
- 18. Any unique identifying number, characteristic or code

A person with appropriate expertise must determine that the risk is very small that the information could be used alone or in combination with other reasonably available information by an anticipated recipient to identify the individual. AND this person must document the methods and justification for this determination.

VIII. Disclosures to Family, Friends or Others-Participant Location

There are instances when a participant's friend or family member contacts Axis to ask about the location of a patient or whether the patient has been seen at Axis. Following is guidance provided to assist staff in providing appropriate responses for specific situations that commonly occur. In rare cases of emergency, at the discretion of senior management the minimum of information my be released in order to assist in resolving and emergency situation.

Guidance

Situation: Friends or family are concerned about the whereabouts of a person. They contact the company to ask if a person is at Axis or has been seen as a participant recently.

Response:

If the person is not currently an Axis participant, the caller may be told that the person is not at the clinic. If the person is currently receiving services at the clinic, clinic staff should take the name of the caller, their purpose for calling the participant and tell them that they will check. Staff should then ask the participant if it is okay to provide information to the caller and what information to provide. If the patient does not want the clinic

staff to provide information, staff should tell the caller that they are unable to provide information about the participant due to privacy rights and suggest that the caller contact the participant directly for information. If the caller is asking for historical information about visits or services provided and the participant has not either provided an authorization to share this information with this person pertaining to their involvement in the patient's treatment or payment, the caller should be informed that due to HIPAA confidentiality requirements, information about participant visits is not provided without participant authorization.

Situation: An individual comes to Axis and tells the reception area that they have arrived to pick up a patient.

Response:

If the participant has notified Axis staff that someone is coming to pick them up (by giving the name of the individual), the individual should be directed to the location of the participant. If the patient has not provided information about anyone coming to pick them up, Axis staff should ask for the person's name and tell the person that they will check. Another staff member should be given a note to tell the participant that someone has arrived to pick them up and ask them whether it is okay to tell the person the participant's location.

IX. Removing PHI from Company Premises

When Axis Community Health deems it necessary for an employee to work from a location other than one of our sites, PHI may be accessed and/or removed under the following circumstances:

- 1. Before removing PHI from Axis for company business you must receive the approval from your department Director and IT.
- 2. Axis will only allow the paper (participant records, reports) removal of PHI when transported in a secure lock box and when approved by the department Director and the Privacy Officer.
- 3. Axis will provide laptop computers for employees *required* to work offsite and access PHI in a non-Axis setting. Any files saved on these computers are saved to the network and are therefore secure.
- 4. Staff members that work at school sites and create paper files at the school are required to keep these files locked securely. While in transit, these files are kept locked in secured carrying cases.
- 5. Staff member with progress notes and other forms that need to be signed by their supervisors can be brought back to Axis in a locked carrying case. These documents can also be saved on the Axis server in a designated secure file on the company network, or on a password-protected flash drive received by IT.
- 6. The electronic removal of PHI (using flash drives) for the purposes of working from a non-Axis setting may be approved in advance by IT only. In the very rare circumstance that it becomes necessary, the PHI should be rigorously safeguarded physically as well as electronically, including *employee-performed* encryption of all files. Most flash drives have the capability to assign a password.

- 7. The following safeguards are required of all employees when working from a non-Axis site:
 - When outside the facility, only work on health information in a secure private environment.
 - Keep the information with you at all times while in transit.
 - Do not permit others to have access to the information.
 - Never email participant information.
 - Don't save participant information to your home computer.
 - Do not print records of any type.
 - Do not record login information on or near the computer.
 - Return all information the next business day or as soon as required.

The Company uses a third party vendor for the daily transportation of paper participant charts from clinic site to clinic site. This vendor is state-licensed, bonded and insured as a Mail Courier Service provider.

Axis Community Health will immediately investigate any incident that involves the loss or theft of PHI that was taken off-site.

X. Faxing PHI

Each fax should be accompanied by an Axis fax cover sheet. Faxing of highly confidential information is not recommended. Faxing of highly confidential information is only permitted if the sender first calls the recipient and confirms that the recipient or his/her designee can be waiting at the fax machine, and then, the recipient or his/her designee waits at the fax machine to receive the fax and then calls the sender to confirm receipt of the document. Both the sender and the recipient must be attentive to the sensitive nature of highly confidential information.

If the fax was transmitted to the wrong recipient, in all cases follow these steps:

Fax a request to the incorrect fax number explaining that the information has been misdirected, and ask that the materials be returned or destroyed. Document the incident on an Incident Report Form and notify the HIPAA Privacy Officer at (925) 201-6038. Verify the fax number with the recipient before attempting to fax the information again.

SECTION 3: Participant Individual Rights

I. Access to Protected Health Information and Requests for Amendment

HIPAA gives participants the right to access and obtain copies of their PHI that the Company or its business associates maintains. HIPAA also provides that participants may request to have their PHI amended. The Company will provide access to PHI and it will consider requests for amendment that are submitted in writing by participants.

II. Accounting

An individual has the right to obtain an accounting of certain disclosures of his or her own PHI. This right to an accounting extends to disclosures made in the last six years, other than disclosures:

- to carry out treatment, payment or health care operations;
- to individuals about their own PHI;
- incident to an otherwise permitted use or disclosure or pursuant to an authorization;
- for purposes of creation of a facility directory or to persons involved in the participant's care or other notification purposes;
- as part of a limited data set; or
- for other national security or law enforcement purposes.

The Company shall respond to an accounting request within 60 days. If the Company is unable to provide the accounting within 60 days, it may extend the period by 30 days, provided that it gives the participant notice (including the reason for the delay and the date the information will be provided) within the original 60-day period.

The accounting must include the date of the disclosure, the name of the receiving party, a brief description of the information disclosed, and a brief statement of the purpose of the disclosure (or a copy of the written request for disclosure, if any).

The first accounting in any 12-month period shall be provided free of charge. The Privacy Officer may impose reasonable production and mailing costs for subsequent accountings. The Privacy Officer is responsible for responding to a request for Accounting.

III. Requests for Alternative Communication Means or Locations

Participants may request to receive communications regarding their PHI by alternative means or at alternative locations. For example, participants may ask to be called only at work rather than at home. Such requests may be honored if, in the sole discretion of Axis, the requests are reasonable.

However, Axis shall accommodate such a request if the participant clearly provides information that the disclosure of all or part of that information could endanger the participant. The Privacy Officer in collaboration with managers has responsibility for administering requests for confidential communications.

IV. Requests for Restrictions on Uses and Disclosures of Protected Health Information

A participant may request restrictions on the use and disclosure of the participant's PHI. It is the Company's policy to attempt to honor such requests if, in the sole discretion of the Company, the requests are reasonable. The Privacy Officer is charged with responsibility for processing requests for restrictions.

V. When a Participant Requests a Copy of his/her Record

A participant can request a copy of his/her medical record by completing a Request for Accessing/Inspecting/Copying Health Information form and submitting it to the Department that maintains the information being requested. The Department in collaboration with the Privacy Officer must process and respond to the request.

Participants can receive this form from Patient Services or by going directly to the department that maintains their records.

VI. Participants Request for copy of Clinic Notes or Labs while Checking out After an Appointment

It's okay to provide a participant with a copy of a clinic note or labs that are maintained in their files. It is recommended that you follow the best practice of stamping or writing "Participant Copy" on <u>each</u> page.

VII. Acceptable Methods of Verification of Identity for Release of Personal Health Information (PHI):

When the Requestor is the Participant

The Company will take reasonable steps and exercise professional judgment to verify the identity of the individual making a request for access to his/her own PHI.

- a. **If the request is made in person**, verification of identity may be accomplished by asking for photo identification (such as a driver's license). A copy of the I.D. must be attached to the request and placed in the Participants record.
- b. **If the request is made over the telephone**, verification will be accomplished by requesting identifying information such as social security number, birth date, and medical record number and confirming that this information matches what is in the participant's record. Or, verification will occur through a callback process using phone numbers documented in the participant record to validate the caller's identity.
- c. **If the request is made in writing,** verification will be accomplished by requesting a photocopy of photo identification if a photocopy of the ID is not available, the signature on the written request must be compared with the signature in the participant record. In addition, Axis will need to verify the validity of the written request by contacting the participant by telephone.

V1II. When the requestor is the Participants Legally Authorized Representative

Verification of identity will be accomplished by asking for a valid photo identification (such as driver's license) if the request is made in person. Once identity is established, authority in such situations may be determined by confirming the person is named in the medical record or in the participant's profile as the participant's legally authorized representative. Or, if there is no person listed in the medical record as the participant's legally authorized representative, authority may be established by the person presenting an original of a valid power of attorney for health care or a copy of a court order appointing the person guardian of the participant and a valid photo I.D. A copy of the I.D. and legal notice must be attached to the request and placed in the Participants record.

IX. Other Methods

The Company may use any other method of verification that, in the Company's discretion, is reasonably calculated to verify the identity of the person making the request. Some acceptable means of verification include, but are not limited to:

- d. Requesting to see a photo ID
- e. Requesting a copy of a power of attorney
- f. Confirming personal information with the requestor such as date of birth, policy number or social security number
- g. Questioning a child's caretaker to establish the relationship with the child
- h. Calling the requestor back through a main organization switchboard rather than a direct number

PHI Breach Reporting

The purpose of this section is to address the Company's privacy requirements for reporting, documenting, and investigating a known or suspected action or adverse event resulting from unauthorized use or disclosure of individually identifiable health information.

A privacy breach is an adverse event or action that is unplanned, unusual, and unwanted that happens as a result of non-compliance with the privacy policies and procedures of the Company. A privacy breach must pertain to the unauthorized use or disclosure of health information, including 'accidental disclosures' such as misdirected e-mails or faxes.

The Privacy Officer shall immediately investigate and attempt to resolve all reported suspected privacy breaches.

Staff members are required to verbally report to his/her supervisor any event or circumstance that is believed to be an inappropriate use or disclosure of a participant PHI. If the supervisor is unavailable, the staff member must notify the Privacy Officer within 24 hours of the incident. If the manager determines that further review is required, the manager and staff member will consult with the Privacy Officer to determine whether the suspected incident warrants further investigation. In all cases and Incident Report must be filled out and submitted to the appropriate reviewer.

The Privacy Officer will document all privacy incidents and corrective actions taken. Documentation shall include a description of corrective actions, if any are necessary, or explanation of why corrective actions are not needed, and any mitigation undertaken for each specific privacy incident. All documentation of a privacy breach shall be maintained with the Privacy Officer and shall be retained for at least six years from the date of the investigation. Such documentation is <u>not</u> considered part of the participant's health record.

If the participant is not aware of a privacy incident, the Privacy Officer shall investigate the incident thoroughly before determining whether the participant should be informed. If the participant is aware of a privacy incident, the Privacy Officer shall contact the participant within three (3) business days of receiving notice of the incident. The method of contact is at the discretion of the Privacy Officer, but resulting communications with the participant must be documented in the incident report. In addition, any privacy incident that includes a disclosure for which an accounting is required must be documented and entered into accounting.

Staff who fail to report known PHI/security incidents, or fail to report them promptly, may be subject to disciplinary action up to termination.

I. Breach Notification Requirements

Following a breach of unsecured protected health information, covered entities must provide notification of the breach to affected individuals if necessary and in certain circumstances, to the media. In addition, business associates must notify covered entities that a breach has occurred.

• Individual Notice

Covered entities must notify affected individuals following the discovery of a breach of unsecured protected health information. Covered entities must provide this individual notice in written form by

first-class mail, or alternatively, by e-mail if the affected individual has agreed to receive such notices electronically. If the covered entity has insufficient or out-of-date contact information for 10 or more individuals, the covered entity must provide substitute individual notice by either posting the notice on the home page of its web site or by providing the notice in major print or broadcast media where the affected individuals likely reside. If the covered entity has insufficient or out-of-date contact information for fewer than 10 individuals, the covered entity may provide substitute notice by an alternative form of written, telephone, or other means.

These individual notifications must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include, to the extent possible, a description of the breach, a description of the types of information that were involved in the breach, the steps affected individuals should take to protect themselves from potential harm, a brief description of what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches, as well as contact information for the covered entity. Additionally, for substitute notice provided via web posting or major print or broadcast media, the notification must include a toll-free number for individuals to contact the covered entity to determine if their protected health information was involved in the breach.

• Media Notice

Covered entities that experience a breach affecting more than 500 residents of a State or jurisdiction are, in addition to notifying the affected individuals, required to provide notice to prominent media outlets serving the State or jurisdiction. Covered entities will likely provide this notification in the form of a press release to appropriate media outlets serving the affected area. Like individual notice, this media notification must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach and must include the same information required for the individual notice.

• *Notice to the Secretary*

In addition to notifying affected individuals and the media (where appropriate), covered entities must notify the Secretary of breaches of unsecured protected health information. Covered entities will notify the Secretary by visiting the HHS web site and filling out and electronically submitting a breach report form. If a breach affects 500 or more individuals, covered entities must notify the Secretary without unreasonable delay and in no case later than 60 days following a breach. If, however, a breach affects fewer than 500 individuals, the covered entity may notify the Secretary of such breaches on an annual basis. Reports of breaches affecting fewer than 500 individuals are due to the Secretary no later than 60 days after the end of the calendar year in which the breaches occurred.

• Notification by a Business Associate

If a breach of unsecured protected health information occurs at or by a business associate, the business associate must notify the covered entity following the discovery of the breach. A business associate must provide notice to the covered entity without unreasonable delay and no later than 60 days from the discovery of the breach. To the extent possible, the business associate should provide the covered entity with the identification of each individual affected by the breach as well as any information required to be provided by the covered entity in its notification to affected individuals.

II. Complaint/Concerns Reporting

Concerns about the Company's privacy practices may arise in a variety of contexts and may be received by many different persons at the Company. It is important that the Company responds to concerns and complaints in a timely manner. When a staff member hears or receives a complaint/concern, he/she should ask the complainant whether or not the complainant wishes to file a formal complaint and offer to assist the complainant with the form. Even if the person does not wish to file a complaint or provide identifying information, the staff member should proceed with the procedures outlined below.

Filing a Complaint

- **a. Participant's** complaints of alleged privacy rights violations may be forwarded through multiple channels, such as telephone calls, letter via mail/email, in person. If these complaints are received by a staff member the person receiving the complaint will:
 - In response to a Telephone Call or In-Person Request to File a Complaint Complete the Privacy Complaint Form and immediately forward to the Privacy Officer. Offer to forward a copy of the complaint form to the complainant.
 - In response to a Letter or Email (print out) Complete the Privacy Complaint Form and immediately forward to the Privacy Officer. Attach the written complaint to the complaint form.
 - In response to an Anonymous Complaint– Complete the Privacy Complaint Form based on the information provided and immediately forward to the Privacy Officer. When possible, explain to the complainant that the Company has an obligation to follow up on complaints whether or not they are anonymously filed.
- b. Staff Members Call the Privacy Officer at (925) 201-6038. Staff members may also complete the Privacy Complaint Form and forward to the Privacy Officer. Staff members can also fill out the complaint form and put it in the Privacy Officers mail box located at 4361 Railroad Avenue, Suite E. Upon receipt of a complaint, the Privacy Officer will initiate primary investigation.
 - Initial review All complaints will be initially reviewed by the Privacy Officer or his/her designee to determine if the complaint alleges a violation of established policies and procedures or other known regulations regarding the protection of individually identifiable health information. If there is no legitimate allegation, the Privacy Officer will, when possible, contact the Complainant by letter and inform him/her of this finding within 60 days. All documentation will be maintained as prescribed in this policy.
 - Complaints requiring further review If there is a legitimate allegation, the Privacy Officer or his/her designee will conduct a detailed investigation by reviewing the covered University unit practices, contacting employees, students, or volunteers as needed, working with the Security Officer (as applicable), and utilizing other University resources as needed. Upon conclusion of the investigation, the Privacy Officer will, when possible, contact the Complainant by letter and inform him/her of the finding within 60 days.
- **c. 60-day time frame** In the event that this 60-day period cannot be met, the Privacy Officer shall, when possible, communicate this determination to the Complainant in writing and include an estimated timeframe for completion of the investigation.

- **d. Outcome of Investigation -** The purpose of the investigation is to determine the compliance of the Company's policies and procedures implementing the privacy standards mandated by HIPAA. The Company will mitigate, to the extent practicable, any harmful effect that is known of a use or disclosure of PHI in violation of the Company's policies and procedures or HIPAA's privacy requirements by the Company or any of its Business Associates. In the event that disciplinary action is recommended, the Privacy Officer or his/her designee will coordinate any action with management.
- **e. Documentation -** All complaints sent to the Privacy Officer shall be documented in a format that includes all of the information contained on the Privacy Complaint Form. The Privacy Officer will maintain all completed complaints' documentation for six years from the initial date of the complaint.

III. Non-Retaliation

The Company shall not intimidate, threaten, coerce, discriminate against, or take any other form of retaliatory action against any person who has reported a privacy incident.



Summary Guidelines for Safeguarding the Privacy of Health Information

These are guidelines centered on how to safeguard health information and ensure confidentiality when using normal business communications, such as conversations, telephone, faxes, mail, and electronic mail. Wherever practical, the material containing Protected Health Information (PHI) should be labeled as confidential on the document, diskette, CD, or other medium. PHI maintained electronically should be password-protected in all media.

Also when using and disclosing PHI, you must take reasonable measures to ensure the information is protected. Below are simple safeguarding tasks that <u>should</u> be used when communicating in a work environment that necessitates access to and use and disclosure of PHI. Remember to limit your communications of PHI to the minimum necessary for the intended purpose. Restrict your communications to those who have a valid "need to know" the information. If you have questions about these safeguards and how to protect PHI communications, please discuss them with your supervisor.

	Courier and Regular Mail
Oral Conversations – in person	☐ Use sealed secured envelopes to send PHI.
☐ Discuss participants PHI in private. Use an office with a door	☐ Verify that the authorized person has received the package.
whenever possible, or leave areas where others can overhear.	☐ Deliver all mail promptly to the recipient.
☐ Be aware of those around you and lower your voice when	☐ Mailboxes must be in safe areas and not located in public or
discussing participants health information.	
☐ If possible, point out health information on paper or on-screen non-	high-traffic areas.
verbally when discussing participants health information.	Inter-Office Mail
Oral Conversations - telephone	□ Put PHI in closed inter-office envelopes. As an added
☐ Follow the above guidelines for "Oral Conversations"-in person"	precaution, put PHI in a sealed envelope inside the inter-office
☐ Don't use names instead say; "I have a question about a client".	envelope.
□ Never give PHI over the phone when talking to unknown callers,	☐ Identify recipient by name and verify mail center address.
but call back and verify information.	☐ Distribute inter-office mail promptly to recipients. Do not leave
☐ Never leave PHI on voice messages; instead leave a message	unattended in mailboxes.
requesting a return call to discuss a participant giving only your name	☐ Where practical, use lockable containers (e.g. attaches) to
and phone number.	transmit correspondence that contains participant PHI.
☐ Do not discuss PHI over unencrypted cellular or portable (wireless)	Computer Workstations
phones or in an emergency, as the transmissions can be intercepted.	☐ Use password protected screen savers, turn off the computer, or
Fax	log out of the network when not at your desk.
\Box Put fax machines in a safe location, not out in the open or in a	☐ Position screens so they are not visible to others.
public or area with high-traffic or easy access and visibility.	☐ Secure workstations and laptops with password.
☐ Use a cover sheet clearly identifying the intended recipient and	☐ Change passwords on a regular basis.
include your name and contact information on the cover sheet.	☐ Do not leave laptop or work-related participant PHI visible or
☐ Include a confidentiality statement on the cover sheet of faxes that	unsecured in a car, home office, or in any public areas.
contain PHI.	☐ Ensure that all PHI used outside work premises is protected
□ Do not include or reference PHI on cover sheet.	using appropriate measures such as locked desks, file cabinets.
☐ Confirm fax number is correct before sending.	☐ Never remove original copies of PHI from the agency without
☐ Send fax containing participant health information only when the	your supervisor's approval for specific purposes.
	☐ Store files that contain PHI on a secure server, not on your
authorized recipient is there to receive it whenever possible.	workstation hard drive.
□ Verify that fax was received by authorized recipient; check the	Disposal of PHI
transmission report to ensure correct number was reached and when	☐ Shred all hard copies containing PHI when the copies are no
necessary contact the authorized recipient to confirm receipt.	longer needed.
☐ Deliver received faxes to recipient as soon as possible. Do not	☐ Place hardcopies to be recycled in locked recycle bins if
leave faxes unattended at fax machine.	available.
Email	☐ Delete all soft copy files containing PHI from your computer and
☐ Do not include PHI in Subject-line or in Body of email.	from the server when the information is no longer needed within
☐ Transmit PHI only in a password-protected attachment (MS Word	the record retention requirements.
and MS Excel provide password protection).	
☐ Include a confidentiality statement on emails that contain any PHI	☐ Destroy all disks, CDs, etc., that contained PHI before disposing
in email attachments.	them.
$\ \square$ Do not send attachment passwords in the same email as the	☐ Do not reuse disks, CDs that contained PHI without sanitizing
attachment.	them first.
☐ Include your contact information (name and phone number	☐ Contact IT before transporting or transferring equipment for
minimum) as part of the email.	proper procedures to move equipment and to sanitize hard drives
☐ Set email sending options to request an automatic return receipt	and other media.
from your recipient(s).	☐ Return the PHI to the sender, if this requirement is stipulated in
☐ Request that email recipients call to discuss specific participant data.	any contractual agreements.
☐ Do not store emails or email attachments with PHI on your hard drive but	Work Areas
copy and store to a secure server. Delete the email and the attachments when	 Do not leave PHI (files, records, Rolodex, reports) exposed, open, or unattended in public areas, conference rooms, mailboxes, wall trays, etc.
they are no longer needed.	□ Store all PHI securely in locked file cabinets, desk drawers, offices, or
	suites when you are not in your work area

AXIS COMMUNITY HEALTH SUMMARY NOTICE OF PRIVACY PRACTICES

THIS IS A SUMMARY OF OUR NOTICE OF PRIVACY PRACTICES, WHICH DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION.

Our pledge to protect your privacy:

Axis Community Health is committed to protecting the privacy of your medical information. Your care and treatment is recorded in a medical record. So that we can best meet your medical needs, we share your medical record with the providers involved in your care. We share your information only to the extent necessary to collect payment for the services we provide, to conduct our business operations, and to comply with the laws that govern health care. We will not use or disclose your information for any other purpose without your permission.

Participant Rights - You have the following rights regarding your medical information:

- to request to inspect and obtain a copy of your medical records, subject to certain limited exceptions;
- to request to add an addendum to or correct your medical record;
- to request an accounting of Axis Community Health's disclosures of your medical information;
- to request restrictions on certain uses or disclosures of your medical information;
- to request that we communicate with you in a certain way or at a certain location;
- and to receive a copy of the full version of our Notice of Privacy Practices.

We may use and disclose medical information about you for the following purposes:

- to provide you with medical treatment and services;
- to bill and receive payment for the treatment and services you receive;
- for functions necessary to run Axis Community Health and assure that our participants receive quality care;
- to provide basic contact information (no medical information is provided) to our development office for purposes of fundraising for Axis Community Health;
- to support our standing as an federally qualified health center;
- and as required or permitted by law.

There are additional situations where we may disclose medical information about you without your authorization, such as:

- for workers' compensation or similar programs;
- for public health activities (e.g., reporting abuse or reactions to medications);
- to a health oversight agency, such as the California Department of Health Services;
- in response to a court or administrative order, subpoena, warrant or similar process;
- to law enforcement officials in certain limited circumstances;
- to a coroner, medical examiner or funeral director; and
- to organizations that handle organ, eye, or tissue procurement or transplantation.

Our Notice may be revised or updated from time to time. Please see our full Notice of Privacy Practices for a more detailed description of our privacy practices, your rights regarding you medical information, and pertinent contact information.

For further information about the full Notice of Privacy Practices, please contact: Axis Community Health's Privacy Officer at (925) 201-6038. A complete version of this notice is available on our website at www.axishealth.org.

AXIS COMMUNITY HEALTH ACKNOWLEDGEMENT OF RECEIPT OF SUMMARY NOTICE OF PRIVACY PRACTICES

Our Notice of Privacy Practices provides information about how we may use and disclose protected health information about you. The notice contains participant rights section describing your rights under the law. You have the right to review our Notice before signing this Consent. The terms of our Notice may change. If we change our Notice, you may obtain a revised copy by contacting our office at (925) 201-6038.

You have the right to request that we restrict how protected information about you is used or disclosed for treatment, payment or health care operations. We are not required to agree to this restriction, but if we do, we shall honor that agreement.

By signing this form you consent to our use and disclosure of protected health information about you for treatment, payment and health care operations. You have the right to revoke the Consent in writing, signed by you. However, such a revocation shall not affect any disclosures we have already made in reliance on your prior Consent. Axis Community Health provides this form to comply with the Health Insurance Portability and Accountability Act of 1996 (HIPPA).

The participant understands that:

- Protected health information may be disclosed or used for treatment, payment or health care operations.
- Axis Community Health has a Notice of Privacy Practices and that the participant has the opportunity to review this notice.
- Axis Community Health reserves the right to change the Notice of Privacy Practices.

the practice's complete Notice of Privacy Practices if I so desire.

Relationship of Participant Representative to Participant

• The participant has the right to request restrictions to the uses of their information but Axis Community Health does not have to agree to those restrictions.

I have received a copy of the Summary Notice of Privacy Practices. I understand that I may also request a copy of

- The participant may revoke this Consent in writing at any time and full disclosures will then cease.
- Axis Community Health may condition receipt of treatment upon the execution of this consent.

Name of Participant (print)

Signature of Participant

Date

Signature of Participant Representative

(Required if participant is a minor or an adult who is unable to sign this form)

Print Name

AXIS COMMUNITY HEALTH

Authorization for Release and/or Disclosure of Health Information

I authorize the disclosure of my personal health information to the persons/entities as described below. I understand this authorization is voluntary, and made to confirm my directions. I understand that once the information is disclosed, it may be re-disclosed and no longer protected by federal privacy regulations. I hereby give permission to Axis Community Health to disclose my personal health information in the manner described herein.

	PARTICIPANT'S	INFORMATION	
Name:		Axis Medical Recor	rd #:
Birthdate:	Contact Phone Number:		Request Date:
	PHI MAY BE DI	ISCLOSED BY:	
Person/Facility:		Phone: Fax #:	
Address:			
	PHI MAY BE DI	SCOLOSED TO	
Person/Facility:		Phone #: Fax: #:	
Address:			
PE	RSONAL HEALTH INFOR	MATION TO BE DIS	SCLOSED
1. Specify records to be released	and /or disclosed:		
☐ General Medical Information (from to)	
□ Information Regarding Specific	c Injury or Treatment (from	to)
□ X-Ray/Laboratory Results of (1	from to)	
□Mental Health (from	to	Initials of Participant	or Representative
□Alcohol/Drug (from	to	_) Initials of Participa	nt or Representative
□HIV Test Results (from	to) In	itials of Participant or	Representative
□ Other (specify):			
-	•	-	asmitted disease, alcohol or drug use or quest, unless you specifically state your
occurred before Axis Community Health revoke it, this authorization will expire of to Axis Community Health, ATTN: Priva	received and processed a written notic ne year from the date of signature below	e of revocation. I understand w. To revoke this authorizat	revocation will NOT affect any disclosures that d that if I did not specify duration and if I do not ion, I understand that I must send a written request
	elease nonpublic personal health inform	nation. I understand that Ax	d I confirm that the contents are consistent with my is Community Health will not condition treatment,
By:Participant's Name (Prin		Ponticiment's Ci	D-4
	lso complete, sign and date below. C		Date s your relationship to the participant. Please
By:Participant's Name (Prin			
	nt) P	Participant's Signature	

AXIS COMMUNITY HEALTH

Request for Alternative Means of Communication of Protected Health Information

Use this form to request that you receive communications of protected health information (PHI) by alternative means, or at an alternate location.

Completing this form is voluntary. However, if you would like alternative means of communication of your protected health information, you must provide all of the information requested on this form. Personally identifiable information requested on this form is mandatory in order to process your request and will only be used for this purpose.

INSTRUCTIONS: Mail or hand deliver this completed form to the following address: Axis Community Health, ATTN: Privacy Officer, 4361 Railroad Avenue, Pleasanton, CA 94566

INDIVIDUAL'S INFORMATION			
Name:		Medical Record # o	r ID#:
Birthdate:	Contact Phone Number:		Request Date:
Current Address (No., street, city, sta	l ite, zip):		
Please read and complete the follow	vina		
At Axis Community Health, we may benefits). Communications are addinformation in your medical records endanger you, you have the right to reasonable alternate means for Send your PHI to an alternate address. Contact you at an alternate phone in Please note that we are not able reasons of convenience.	ay mail communications coressed to your address as when we contact you by equest that we: or communicating your PHI ess umber to accommodate requests	listed in our medicatelephone. If you bel	o the subscriber (the person receiving the all records. We also rely upon telephone ieve this method of communication could be to alternate addresses made solely for
	LTERNATIVE MEANS		
I request that Axis Community Healt to an alternate address, and/or to con alternate means, address, phone num	tact me at an alternate phone	e number. (Please prov	e means, to send such communications vide full information regarding the
I hereby request that any future communication directed through alternate methods or	nunications to me from Axi		regarding my health information be
☐ Alternative Phone Numb	per: ()		
☐ Alternative Mailing Add	ress: ()		
☐ Other Alternative Means	3:		
State any harm that may occur if this	request is denied:		

ACKNOWLEDGEMENT

Please sign and date:

			that Axis Community Health is not required to agree odate reasonable request when appropriate.	e to every accommodation
By:				
	Participant's Name (Print)	Participant's Signature	Date
			nplete, sign and date below. Check the box that de r relationship tot the participant (e.g. Power of At	
By:				
	Participant's Name (Print)	Participant's Signature	Date
		This !	Section for Company Use Only	
	Request APPROVED			
			vidual. Send original to Medical Records to make ssociate(s) as needed.	amendment and place in
	Request DENIED			
	Reason for Denial:	☐ Admini	pensive to accommodate request stratively impractical to accommodate request of Participant to specify an alternative accommodation	on
	Send a copy of complete file.		ial. Send original to Medical Records to place in indi	
	Date copy sent:		Copy sent by (print name:	

AXIS COMMUNITY HEALTH Request for Accessing/Inspecting/Copying Health Information

As required by the Health Information Portability and Accountability Act of 1996 (HIPAA) you have a right to request the opportunity to inspect and copy health information that pertains to you. Axis Community Health will evaluate your request and will either grant it or explain the reason why the request will not be granted. Axis Community Health may provide you with a summary or explanation of the information in your health plan records instead of access to or copies of your records.

Mail or hand deliver this completed form to: Axis Community Health, ATTN: Privacy Officer, 4361 Railroad Avenue, Pleasanton, CA 94566

CA 7+300	INDIVIDUAL'S I	NFORMATION		
Name:		Medical Record # or I	D#:	
Birthdate:	Contact Phone Number:		Request Date:	
Current Address (No., street, cit	zy, state, zip):		l	
	REQUEST TO ACCES			
	mation in the following designated to		eriod of time from	
Medical RecordsEnrollment, payment, or	□ laboratory Reports □ Ficlaims adjudication information med record sets:	nancial Records	_	
	DELIVERY 1			
Please check the box indicatin	g how you would like to receive	the requested health i	records.	
□ mail to my current address:	street address	city sta	ate zip code	
	street address	City Sta	ate zip code	
	to provide photo identification.) lap		number where we may con	ntact you
	e required to provide photo identif f member. Please provide a phone			
ACKNOWLEDGEMENT Please sign and date: I understand that certain exceptions, you have the right to However, you do not have a right to ins proceedings and records that are subjective.	mstances when a licensed health care prof	nformation in a designated rea tes or information compiled t	cord set maintained by Axis Cor for civil, criminal, or administra	nmunity Health. tive action or
By:				
By:Participant's Name (Pr	int) Pa	articipant's Signature		Date
participant. Please attach pro	please complete, sign and date of or your relationship to the pa			
By:Participant's Name (Pr	int) Pa	articipant's Signature		Date
	gal Guardian □Power of Attor		ther	

This Section for Company Use Only

Determination:		REQUEST APPROVED. Approved date:		
Agency Responsibilities:		Determination of method for Participant access. Determination date:		
8		Notice to Participant of approved access. Sent date:		
		Offer Participant summary of information. Sent date:		
		Notify Participant of requirements for copies of health information. Sent date:		
Determination:		REQUEST NEEDS FURTHER REVIEW		
	Designated	Staff Date		
Review of Request by Lic	ensed H	ealth Care Professional		
Determination:		REQUEST APPROVED. Approved date:		
Agency Responsibilities:		Determination of method for Participant access. Determination date:		
rigency responsionates.		Notice to Participant of approved access. Sent date:		
		Offer Participant summary of information. Sent date:		
		Notify Participant of requirements for copies of health information. Sent date:		
		Trouty I with pull of requirements for copies of neutral missing and being duty		
Determination:		REQUEST DENIED. Denial date:		
Reason for Denial:		Reference made to another person could endanger that person		
		Access could endanger life or physical safety of Participant or other(s)		
		Access requested by personal representative and access could cause substantial harm to Participant		
		or other(s)		
		Other		
Agency Responsibilities:		Written Notice to Participant of basis for denial. Sent date:		
Tigeney nesponsioniues.		Provide Participant with Opportunity to Request Review by licensed health care professional		
		Sent date:		
Licensed H	ealth Care	Professional Date		
Request Second Review				
Determination:		REQUEST APPROVED		
A D 11.11%				
Agency Responsibilities:		Determination of method for Participant access		
		Notice to Participant of approved access Offer Participant summary of information		
		*		
		Notify Participant of requirements for copies of health information		
Determination:		REQUEST DENIED		
Reason for Denial:		Reference made to another person could endanger that person		
Trousen for Bennan	ā	Access could endanger life or physical safety of Participant or other(s)		
	_	Access requested by personal representative and access could cause substantial harm to Participant		
	_	or other(s)		
		Other		
Agency Responsibilities:		Written Notice to Participant of basis for denial. Sent date:		
		<u></u>		
Licensed F	Health Care	Professional Date		

AXIS COMMUNITY HEALTH Request for Amendment of Health Information

As a participant in Axis Community Health's services you have the right to request amendments to your personal health information that are inaccurate or incomplete. If you want to amend your health information, you must complete this form and return it to Axis Community Health, ATTN: Privacy Officer, 4361 Railroad Avenue, Pleasanton, CA 94566

If we deny your request, we will let you know in writing with an explanation of why we are denying it. You have the right to submit a written disagreement to our denial. We will put your statement and requested amendment in to your record. If we continue to disagree with your amendment request, we may put a written rebuttal to your disagreement into your record. If this occurs, we will let you know in writing and send you a copy of our rebuttal.

	INDIVIDUAL'S IN	NFORMATIO	N	
Name: Medical Record # or ID#:				
Birthdate:	Contact Phone Number:		Request Date:	
Current Address (No., street, cit	y, state, zip):			
	REQUESTED A	MENDMENT		
1. Date(s) of Entry to be amended	ed/corrected:			
2. Type(s) of Entry to be amend	ed/corrected:			
3. Please explain how the entry(s) is incorrect or incomplete:			
4 337 (1 11.1 () ()				
4. What should the entry(s) say	in order to be accurate or complet	e:		
5. Would you like this amendment	ent sent to anyone to whom we ma	y have disclos	ed information to in the past?	□NO □YES
If so, please specify the name ar	nd address of the organization or i	ndividual:		
ACKNOWLEDGEMENT				
Please sign and date:				
By:				
Participant's Name (Pr	int) Pa	rticipant's Sign	nature	Date
	please complete, sign and date of or your relationship to the pa			
By:				
Participant's Name (Pr	int) Pa	rticipant's Sign	nature	Date
□Parent of Minor Child □Le	gal Guardian □Power of Attor	ney Execut	or □Other	

	This Section	for Company Use Only
Amendment has been	: □ Accepted □ Denied (If	denied, check the reason for denial):
□ PHI is not p □ Federal/Stat	ted Health Information) wart of the participant's des te law forbids making corrected tate and complete	<u> </u>
Comments of Axis Pro	ovider:	
Amendment has been Date	reviewed by the following Please Print Name	Provider(s): Signature of Provider
Date	Please Print Name	Signature of Provider
Notification was sent	to the Participant on:	Date
Send a copy of completed file.	form to individual. Send origin	nal to Medical Records to place in individuals Medical Records
Date copy sent:	Copy s	sent by (print name:

<u>AXIS COMMUNITY HEALTH</u> Request for Restrictions on Use and Disclosure of Health Information

You have the right to request that we restrict how protected health information about you is used or disclosed for treatment, payment, or healthcare operations. We are not required to agree to this request for restriction in whole or in part, but if we do, we are bound by our agreement. Any restriction we accept will not apply when the restricted information is needed to provide you with emergency treatment. This agreement does not apply if release is required by law or if it's against any public health requirements. We further have the right to terminate any agreed upon restriction by informing you of the termination in writing. Any such termination will only apply to information created or received after we have informed you of the termination.

Please complete this form to request a restriction and return it to Axis Community Health, ATTN: Privacy Officer, 4361 Railroad Avenue, Pleasanton, CA 94566. We will notify you of our ability to comply with your request by returning a copy of this form to you. You also have the right to request us to terminate a restriction to the extent that such termination applies to information created or received after the date of termination.

created of received after		DIVIDUAL'S INFORM	ATION	
Name:		Medical Record # or ID#:		
Birthdate:	Contact Ph	none Number:	Request Date:	
Current Address (No.,	street, city, state, zip):			
	R	ESTRICTIONS REQUE	STED	
1. I would like use and	disclosure of the followi	ng health information to b	e restricted:	
2. I want the information	on restricted because:			
Check the box that tells	s how you want this infor	rmation to be restricted and	d complete the blank:	
□ I do not want this inf	formation to be given to t	he following person(s) or	agency(s):	
0.1	. 1			
☐ Other restrictions req	uested:			
 ACKNOWLEDGEME	NT	_		
Please sign and date:				
By:				
Participant's Na	ame (Print)	Participant'	s Signature	Date
			heck the box that describes you (e.g. Power of Attorney, legal	
Ву:			~.	
Participant's Na Parent of Minor Chile		Participant' Power of Attorney DE		Date

This Section for Company Use Only					
Request has been: ☐ Accepted ☐ Denied (If denied, check the reason for denial):					
Comments of Axis Provider:					
Restriction Request has been reviewed by the following Provider(s):					
Date	Please Print Name	Signature of Provider			
Date	Please Print Name	Signature of Provider			
Notification was sent to the Participant on:					
		Date			
Send a copy of completed form to individual. Send original to Medical Records to place in individuals Medical Records file. Date copy sent: Copy sent by (print name:					

AXIS COMMUNITY HEALTH

Accounting of Non-Authorized Use or Disclosure Request Form

The HIPAA Privacy Regulations allow an individual to request an accounting of certain disclosures of his/her Protected Health Information (PHI). Axis Community Health may disclose your PHI for treatment, payment, health care operations, and as required or permitted by the HIPAA Privacy Regulation or other state or federal laws. Our Privacy Notice informs you that these disclosures may occur without your consent at the time they are made.

You can request an accounting of certain disclosures only about yourself, unless you are authorized to obtain information about another individual. Please complete this form to request a disclosure and return it to Axis Community Health, ATTN: Privacy Officer, 4361 Railroad Avenue, Pleasanton, CA 94566.

ATTN: Privacy Officer, 4361 Railroa	ad Avenue, Pleasanton, CA	94566.	•			
INDIVIDUAL'S INFORMATION						
Name:		Medical Record # or ID#:				
Birthdate: Contact Phone Number:		Request Date:				
Current Address (No., street, city, st	rate, zip):					
	DISCLOSURE	REQUESTED				
disclosures of my protected health in	in the following form: (che	osures only pertaining	to:			
☐ I want to pick up the accounting. Please call me at the following telep	phone number when it is read	dy:				
such additional accounting in advan	additional accountings withice and will be provided with that Axis Community Heal	n the same 12 month in the opportunity to w	this information within the last 12 period. I will be informed of the cost for ithdraw or modify the request in order to ccounting of disclosures within 60 days,			
I understand that Axis Community I	Health does not have to tell 1	me about the following	g types of disclosures:			
 Disclosures made prior to April 14, 2 Disclosures made as part of a limited law. 	data set for purposes of research		Ith care operations, as permitted by federal			

- 3. Disclosures made for purposes of treatment, payment and health care operations.
- 4. Disclosures made to me or disclosures consented to or authorized by me.
- 5. Disclosures made to persons involved in my care.
- 6. Disclosures made for national security or intelligence purposes.
- 7. Disclosures made to correctional institutions or law enforcement officials, under certain circumstances.
- 8. Disclosures made incident to a use or disclosure otherwise permitted or required by law.
- I also understand that my right to an accounting of some or all disclosures may be suspended by the government under limited circumstances.

ACKNOWLEDGEMENT Please sign and date: By: Participant's Name (Print) Participant's Signature Date If you are not the participant, please complete, sign and date below. Check the box that describes your relationship to the participant. Please attach proof or your relationship to the participant (e.g. Power of Attorney, legal guardian) By: __ Participant's Name (Print) Participant's Signature Date □Parent of Minor Child □Legal Guardian □Power of Attorney □Executor □Other Request Determination on Reverse Side This Section for Company Use Only **Privacy Officer Action/Comments:** Action must be taken within 60 days of the receipt of the request Request has been: \square Accepted \square Denied (If denied, please explain): **Comments of Axis Provider:** Disclosure Request has been reviewed by the following Provider(s): Signature of Provider Date **Please Print Name** Date **Please Print Name Signature of Provider** Notification was sent to the Participant on: __ Date Send a copy of completed form to individual. Send original to Medical Records to place in individuals Medical Records file.

_____ Copy sent by (print name: ___

Date copy sent: __

AXIS COMMUNITY HEALTH BUSINESS ASSOCIATE AGREEMENT

This Agreement ("Agreement") is made and entered into this day of <u>Mo</u>	onth:	, Year	by and between
Axis Community Health ("Covered Entity"), whose business address is	4361	Railroad Avenue, Pleasanto	n, CA 94566 and
Business Name:	("Bus	iness Associate"), Type of E	Entity:
	<u> </u>	, whose business address is A	Address of Business
Associate:		_	

- 1. **Definitions.** Terms used, but not otherwise defined in this Agreement, shall have the same meaning as those terms in the Privacy Rule and the Security Rule.
 - a. **Business Associate**. "Business Associate" shall mean [Name of Business Associate].
 - b. **Covered Entity**. "Covered Entity" shall mean Axis Community Health.
 - c. Individual. "Individual" shall have the same meaning as the term "individual" in 45 CFR §160.103 and shall include a person who qualifies as a personal representative in accordance with 45 CFR §164.502(g).
 - d. **Privacy Rule**. "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Part 160 and Part 164, Subparts A and E.
 - e. **Protected Health Information**. "Protected Health Information" shall have the same meaning as the term "protected health information" in 45 CFR §160.103, limited to the information created or received by Business Associate from or on behalf of Covered Entity.
 - f. **Required By Law**. "Required By Law" shall have the same meaning as the term "required by law" in 45 CFR §164.103.
 - g. **Secretary**. "Secretary" shall mean the Secretary of the Department of Health and Human Services or his or her designee.
 - h. **Security Rule**. "Security Rule" shall mean the Standards for Security of Electronic Protected Health Information at 45 C.F.R. parts §160 and §164, subparts A and C.

2. Obligations and Activities of Business Associate.

- a. Business Associate agrees to not use or disclose Protected Health Information other than as permitted or required by this Agreement or as Required by Law.
- b. Business Associate agrees to use appropriate safeguards to prevent use or disclosure of the Protected Health Information other than as provided for by this Agreement. Business Associate agrees to implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of any electronic Protected Health Information that Business Associate creates, receives, maintains or transmits on behalf of Covered Entity, as provided for in the Security Rule.
- c. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by Business Associate in violation of the requirements of this Agreement.
- d. Business Associate agrees to report to Covered Entity any use or disclosure of the Protected Health Information not provided for by this Agreement of which it becomes aware. Business Associate also

agrees to report to Covered Entity any security incident, including all data breaches whether internal or external, related to Protected Health Information of which Business Associate becomes aware.

- e. Business Associate agrees to ensure that any agent, including a subcontractor, to whom it provides Protected Health Information received from, or created or received by Business Associate on behalf of, Covered Entity, agrees to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information.
- f. Business Associate agrees to provide access, at the request of Covered Entity and during normal business hours, to Protected Health Information in a Designated Record Set to Covered Entity or, as directed by Covered Entity, to an Individual in order to meet the requirements under 45 CFR §164.524, provided that Covered Entity delivers to Business Associate a written notice at least five (5) business days in advance of requesting such access. This provision does not apply if Business Associate and its employees, subcontractors and agents have no Protected Health Information in a Designated Record Set of Covered Entity.
- g. Business Associate agrees to make any amendment(s) to Protected Health Information in a Designated Record Set that the Covered Entity directs or agrees to pursuant to 45 CFR §164.526, at the request of Covered Entity or an Individual. This provision does not apply if Business Associate and its employees, subcontractors and agents have no Protected Health Information from a Designated Record Set of Covered Entity.
- h. Unless otherwise protected or prohibited from discovery or disclosure by law, Business Associate agrees to make internal practices, books, and records, including policies and procedures, relating to the use or disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of, Covered Entity, available to the Covered Entity or to the Secretary for purposes of the Secretary determining Covered Entity's compliance with the Privacy Rule or Security Rule. Business Associate shall have a reasonable time within which to comply with requests for such access and in no case shall access be required in less than five (5) business days after Business Associate's receipt of such request, unless otherwise designated by the Secretary.
- i. Business Associate agrees to maintain necessary and sufficient documentation of disclosures of Protected Health Information as would be required for Covered Entity to respond to a request by an Individual for an accounting of such disclosures, in accordance with 45 CFR §164.528.
- j. On request of Covered Entity, Business Associate agrees to provide to Covered Entity documentation made in accordance with this Agreement to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 C.F.R.§164.528. Business Associate shall have a reasonable time within which to comply with such a request from Covered Entity and in no case shall Business Associate be required to provide such documentation in less than five (5) business days after Business Associate's receipt of such request.
- k. Except as provided for in this Agreement, in the event Business Associate receives an access, amendment, accounting of disclosure, or other similar request directly from an Individual, Business Associate will redirect the Individual to the Covered Entity.

3. Permitted Uses and Disclosures by Business Associate.

a. Except as otherwise limited by this Agreement, Business Associate may make any uses and disclosures of Protected Health Information necessary to perform its services to Covered Entity and otherwise meet its obligations under this Agreement, if such use or disclosure would not violate the Privacy Rule if done by Covered Entity. All other uses or disclosures by Business Associate not authorized by this Agreement or by specific instruction of Covered Entity are prohibited.

- b. Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.
- c. Except as otherwise limited in this Agreement, Business Associate may disclose Protected Health Information for the proper management and administration of the Business Associate, provided that disclosures are Required By Law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as Required By Law or for the purpose for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.
- d. Except as otherwise limited in this Agreement, Business Associate may use Protected Health Information to provide Data Aggregation services to Covered Entity as permitted by 45 CFR §164.504(e)(2)(i)(B).
- e. Business Associate may use Protected Health Information to report violations of law to appropriate Federal and State authorities, consistent with §164.502(j)(1).

4. Obligations of Covered Entity.

- a. Covered Entity shall notify Business Associate of any limitation(s) in its notice of privacy practices of Covered Entity in accordance with 45 CFR §164.520, to the extent that such limitation may affect Business Associate's use or disclosure of Protected Health Information.
- b. Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by Individual to use or disclose Protected Health Information, to the extent that such changes may affect Business Associate's use or disclosure of Protected Health Information.
- c. Covered Entity shall notify Business Associate of any restriction to the use or disclosure of Protected Health Information that Covered Entity has agreed to in accordance with 45 CFR §164.522, to the extent that such restriction may affect Business Associate's use or disclosure of Protected Health Information.

5. Term and Termination.

- a. <u>Term.</u> The Term of this Agreement shall be effective as of <u>[Effective Date]</u>, and shall terminate when all of the Protected Health Information provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if it is infeasible to return or destroy Protected Health Information, protections are extended to such information, in accordance with the termination provisions in this Agreement.
- b. <u>Termination for Cause.</u> Upon Covered Entity's knowledge of a material breach by Business Associate, Covered Entity shall give Business Associate written notice of such breach and provide reasonable opportunity for Business Associate to cure the breach or end the violation. Covered Entity may terminate this Agreement, and Business Associate agrees to such termination, if Business Associate has breached a material term of this Agreement and does not cure the breach or cure is not possible. If neither termination nor cure is feasible, Covered Entity shall report the violation to the Secretary.

c. Effect of Termination.

1. Except as provided in paragraph (2) of this section, upon termination of this Agreement for any reason, Business Associate shall return or destroy all Protected Health Information received from, or created or received by Business Associate on behalf of, Covered Entity. This provision shall apply to Protected Health Information that is in the

possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the Protected Health Information.

2. In the event that Business Associate determines that returning or destroying the Protected Health Information is infeasible, Business Associate shall provide to Covered Entity, within ten (10) business days, notification of the conditions that make return or destruction infeasible. Upon such determination, Business Associate shall extend the protections of this Agreement to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such Protected Health Information.

6. Miscellaneous.

- a. <u>Regulatory References.</u> A reference in this Agreement to a section in the Privacy Rule or Security Rule means the section as in effect or as amended.
- b. <u>Amendment.</u> The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Covered Entity to comply with the requirements of the Privacy Rule or Security Rule and the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191.
- c. <u>Survival.</u> The respective rights and obligations of Business Associate under Section 5(c) of this Agreement shall survive the termination of this Agreement.
- d. <u>Interpretation.</u> Any ambiguity in this Agreement shall be resolved to permit Covered Entity to comply with the Privacy Rule or the Security Rule.
- 7. **Counterparts.** This Agreement may be executed in any number of counterparts, each of which shall be deemed an original, but all of which together shall constitute one original Agreement. Facsimile signatures shall be accepted and enforceable in lieu of original signatures.

APPROVED AND ACCEPTED BY:		
Business Associate Print Name & Title	Signature	Date
Axis CEO Print Name	Signature	Date



Confidential Fax

То:			From:		
Fax:			Fax:		
Phone:			Phone:		
Re:			Date:		
Pages:			CC:		
□ Urgent	☐ For Review	☐ As Requested	☐ Please Reply	☐ For Your Records	
• Comment	is:				

IMPORTANT: This facsimile transmission contains confidential information, some or all of which may be protected health information as defined by the federal Health Insurance Portability & Accountability Act (HIPAA) Privacy Rule. This transmission is intended for the exclusive use of the individual or entity to whom it is addressed and may contain information that is proprietary, privileged, confidential and/or exempt from disclosure under applicable law. If you are not the intended recipient (or an employee or agent responsible for delivering this facsimile transmission to the intended recipient), you are hereby notified that any disclosure, dissemination, distribution or copying of this information is strictly prohibited and may be subject to legal restriction or sanction. Please notify the sender by telephone (number listed above) to arrange the return or destruction of the information and all copies.

AXIS INCIDENT REPORT

Date of Incident:	Time of Incident:	am/pm
Axis Location:		
Person(s) Involved Name:(Circle one) Participant Staff Volunteer Contractor Other	If Participant MR#	
Witness(es)		
NATURE OF INCIDENT (check all that apply): O HIPAA Violation/Breach of Confidentiality O Complaint/Grievance O Equipment / Supplies O Facility Safety and Security O Inappropriate Behavior Notified: Police Fire Ambulance Licensing Axis Provider	Injury (specify type) Medication error Medical Emergency Property Damage/TheftOther COO Human Resources	
DETAILS OF INCIDENT (include all known facts, personal states).	sons involved, statements, cause, witnesses, tir	me, location)
RESOLUTION (if applicable)		
REPO Note: Incidents must be reported within 24 hours to department supervisor > COO or HR/Privacy (2 0	must be given
Incident Reported to:	Title:	
Date:		
Report completed by:	Title:	
Date: Contact Phone number:	Dept.:	

OFFICIAL REVIEW

Incident revie	wed by:				
 Safety 	y Assurance Committee Committee n Resources	0 0	Medical Director COO Other		
If applicable	, Severity of HIPAA Privacy	Incident:			
□ Severe	Press may be involved. Affects pagovernment.	rticipant and/or public	ic, business associates, and/or state and/or local		
□ Moderate	□ Moderate Press involvement unlikely. Affects participant and/or business associates.				
□ Low	No affect outside of company. Company able to resolve				
COMMENT	S BY REVIEWER(S):				
RESOLUTIO	ON/CORRECTIVE ACTIO	N:			
☐ Staff Training N☐ Inform Participa	$ \begin{array}{ccc} \text{feeded} & & \Box \text{ Proced} \\ \text{int} & & \Box \text{ Record} \\ \end{array} $	lures to be Reviewed I disclosure in accounting tes log with Privacy Offi			
o No further	r action required, ok to file				
Signature:		Title	Date:		

AXIS COMMUNITY HEALTH COMPLAINT REPORT

Today's Date:	
All information can be submitted anonymously, any identifying	g information is not required.
Name (Optional):	Medical Record #:
Address:	Phone Number:
If you are filing a complaint on someone's behalf, provide the Name:	name and address of the person on whose behalf you are filing.
Address:	
Please describe in detail the nature of your complaint, in names of any Axis staff member and other witnesses (att	ncluding the date or dates of the incident(s), and the name tach additional sheets if necessary):
Participant or Legal Representatives' Signature	Date
Relationship (if not Participant)	Send to: Axis Community Health Privacy Officer, 4361 Railroad Ave., Pleasanton, CA 94566 Fax: 925-417-1503
For Internal Use Only:	
Manager's acknowledgement of receipt Print Name: Date received://	
Process of Investigation:	
Formal Action Taken/Resolution:	
COO or Privacy Office Comments:	
COO or Privacy Officer Signature	
If COO place in QA File, If for Privacy Officer place in HIPA	A Log Binder

FEDERAL & STATE PRIVACY LAWS

Resources from: http://ohii.ca.gov/privacy360/PrivacyLaws/StatePrivacyLaws.aspx

State

California Constitution Article 1 Declaration of Rights:

The California Constitution provides all Californians with a guaranteed right to privacy. http://www.leginfo.ca.gov/.const/.article_1

Confidentiality of Medical Information Act - Civil Code § 56.10-56.16:

This law protects the privacy of medical information by limiting disclosures of providers of health care, health care service plans, and contractors.

http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=00001-01000&file=56.10-56.16

Civil Penalties for Unauthorized Access, Use, or Disclosure of Medical Information - Civil Code § 56.36:

This law was amended to further define administrative fines or civil penalties for any person or entity including licensed health care professionals who knowingly and willfully obtains, discloses, or uses medical information in violation of the Confidentiality of Medical Information Act.

http://www.leginfo.ca.gov/cgi-bin/waisgate?WAISdocID=7175537320+1+0+0&WAISaction=retrieve

Health Facilities Data Breach - Health & Safety Code § 1280.15:

This law requires certain health facilities to prevent unlawful or unauthorized access to, or use or disclosure of, a participant's medical information. It sets fines and notification requirements for breaches of participant medical information and requires facilities to report such breaches to the California Department of Public Health.

http://www.leginfo.ca.gov/cgi-bin/displaycode?section=hsc&group=01001-02000&file=1275-1289.5

Establishment of CA OHII to Ensure Enforcement of Confidentiality of Medical Information – Health & Safety Code § 130201:

This law establishes within the California Health and Human Services Agency the Office of Health Information Integrity to ensure the enforcement of state law mandating the confidentiality of medical information. The law requires every provider to establish and implement safeguards to protect the privacy of participants' medical information.

http://www.leginfo.ca.gov/cgi-bin/displaycode?section=hsc&group=130001-131000&file=130200-130205

Medical Information, Collection for Direct Marketing Purposes - Civil Code § 1798.91:

This law prohibits a business from seeking to obtain medical information from an individual for direct marketing purposes without, (1) clearly disclosing how the information will be used and shared, and (2) getting the individual's consent. http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798.91

Participant Access to Health Records - Health & Safety Code § 123100 :

With minor limitations, this law gives participants the right to see and copy information maintained by health care providers relating to the participants' health conditions. The law also gives participants the right to submit amendments to their records, if the participants believe that the records are inaccurate or incomplete.

http://www.leginfo.ca.gov/cgi-bin/displaycode?section=hsc&group=123001-124000&file=123100-123149.5

Breach Notification - Civil Code § 1798.29 & 1798.82:

This law requires companies that collect personal information to notify each person in their database should there be a security breach involving personal information such as their Social Security number, driver's license number, account number, credit or debit card number, or security code or password for accessing their financial account.

This section defines "personal information" which includes medical information and health insurance information. It defines "medical information" as any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional. The provision defines "health insurance information" as any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.

http://www.leginfo.ca.gov/cgi-bin/waisgate?WAISdocID=39552020520+6+0+0&WAISaction=retrieve

Disclosures of Alcohol and drug information - Health & Safety § 123125:

This chapter does not require a health care provider to permit access to alcohol and drug abuse records that is prohibited by federal and other laws. Records subject to those laws are subject to this chapter to the extent that disclosure is permitted. This chapter does not require a health care provider to allow access of records of communicable disease carriers that is prohibited by law to protect confidentiality.

http://www.leginfo.ca.gov/cgi-bin/waisgate?WAISdocID=39558820827+0+0+0&WAISaction=retrieve

Confidential communication between a victim and a sexual assault counselor - Evidence Code § 1035.8:

A victim of a sexual assault, whether or not a party, has a privilege to refuse to disclose, and to prevent another from disclosing, a confidential communications between the victim and a sexual assault counselor if the privilege is claimed by holder of privilege, person authorized by holder, or sexual assault counselor.

http://www.leginfo.ca.gov/cgi-bin/waisgate?WAISdocID=39562220858+0+0+0&WAISaction=retrieve

Communication between a participant and an educational psychologist. Evidence Code §1010.5 – 1012:

A communication between a participant and an educational psychologist shall be privileged to the same extent, and subject to the same limitations, as a communication between a participant and a psychotherapist http://www.leginfo.ca.gov/cgi-bin/waisgate?WAISdocID=70189111430+0+0+0&WAISaction=retrieve

Lab Results STD - Health & Safety Code §120705:

All laboratory reports for prenatal syphilis tests are confidential and not available for public inspection http://www.leginfo.ca.gov/cgi-bin/waisgate?WAISdocID=39567820967+0+0+0&WAISaction=retrieve

Disclosures of lab for prenatal care: determination of rhesus (Rh) blood type - Health & Safety Code §125105:

A blood specimen obtained as per 125080, shall be submitted to a laboratory to determine rhesus blood type and the results shall be reported to physician, surgeon, or other person providing prenatal care or attending the woman at the time of delivery, and to the woman tested. A blood specimen as per 125080 shall also be submitted to a laboratory to determine the presence of hepatitis B surface antigen and HIV virus. Both results shall be reported to the physician, surgeon, or other person who ordered the test and who shall inform the woman tested. The blood specimen and test results obtained per Health & Safety Code 125085 shall be confidential and not disclosed, unless otherwise provided by law; no person shall be compelled to provide test results pursuant to 125080 or 125085

http://www.leginfo.ca.gov/cgi-bin/waisgate?WAISdocID=39570021035+1+0+0&WAISaction=retrieve

Consent by participant for lab results via internet or other electronic means must be consistent with CMIA – Health & Safety Code §123148:

If the participant requests, a health care provider shall provide the results of the laboratory test to the participant in written or oral form. Consent must be obtained to deliver results via electronic means. Electronic delivery or results shall be consistent with applicable federal law or state law. HIV antibody test, hepatitis infection tests, abusing the use of drugs, and tests related to routinely processed tissues revealing malignant results may not be conveyed by electronic means. Test results and health information may not be used for commercial purpose without participant consent.

http://www.leginfo.ca.gov/cgi-bin/waisgate?WAISdocID=39572921129+0+0+0&WAISaction=retrieve

Lab test results of prisoners – Penal Code §7530:

HIV/AIDS/hepatitis test results for inmate are to be sent to the medical officer ordering them; the laboratory is responsible for ensuring the confidentiality of test results.

http://www.leginfo.ca.gov/cgi-bin/waisgate?WAISdocID=39575521188+1+0+0&WAISaction=retrieve

HIV data used in investigations, reports - Health & Safety Code §120820:

Personal data contained in CAP investigations, reports, and information relating to such must be kept confidential and protected pursuant to 100330. If participant-identifying information is subpoenaed, the department must seek a protective order. The court may still order production of information, but limit it to assure confidentiality.

http://www.leginfo.ca.gov/cgi-bin/waisgate?WAISdocID=39577721244+0+0+0&WAISaction=retrieve

Mandated Blood Testing and Confidentiality to Protect Public Health - Health & Safety Code § 120975-121020:

This law protects the privacy of individuals who are the subject of blood testing for antibodies to the probable causative agent of acquired immune deficiency syndrome (AIDS). No person shall be compelled to provide information in any civil, criminal, administrative, legislative or other proceedings that would reveal the identity of any individual who is the subject of an HIV blood test. Exceptions are provided in Health & Safety Code 1603.1, 1603.3 and 121022.

http://www.leginfo.ca.gov/cgi-bin/waisgate?WAISdocID=39580121282+2+0+0&WAISaction=retrieve

Disclosures by State or Local Public Health agencies of records relating to HIV or AIDS - Health & Safety Code §121025:

HIV or AIDS related public health records containing personally identifying information, developed or acquired by public health agencies shall be confidential and not disclosed except as otherwise provided by law for public health purposes or with written authorization from the person who is the subject of the record or their guardian or conservator. http://www.leginfo.ca.gov/cgi-bin/waisgate?WAISdocID=39580121282+7+0+0&WAISaction=retrieve

Disclosures of medical information regarding the HIV, hepatitis B, or hepatitis C status of the source participant. – Health & Safety Code § 121065:

Test results for AIDS, AIDS-related conditions, and other communicable diseases shall be sent to the designated recipients with a confidentiality disclaimer: "Medical information regarding the HIV, hepatitis B, or hepatitis C status of the source participant

shall be kept confidential and may not be further disclosed, except as otherwise authorized by law." The exposed individual shall also be informed of the penalties for disclosure for which he or she would be personally liable.

http://www.leginfo.ca.gov/cgi-bin/waisgate?WAISdocID=39584221552+0+0+0&WAISaction=retrieve

HIV-related tests requested by insurers – Insurance Code § 799.03:

No life or disability income insurer shall test for HIV without obtaining applicant's informed consent, and providing counseling and privacy protection. In the event of a positive test, the insurer shall notify the applicant's designated physician. http://www.leginfo.ca.gov/cgi-bin/waisgate?WAISdocID=39589021673+0+0+0&WAISaction=retrieve

Confidentiality of AIDS testing for convicted persons - Penal Code § 1202.6:

Upon conviction for prostitution, a court shall order defendant to undergo HIV testing and a report shall made available to the court and State Department of Health Services. At the sentencing hearing, the court shall furnish a copy of the test results to the defendant. Reports of the test results shall be confidential, although Department of Health Services shall furnish copies of any report to a district attorney upon request.

http://www.leginfo.ca.gov/cgi-bin/waisgate?WAISdocID=39592221767+0+0+0&WAISaction=retrieve

Confidentiality of State Department of Mental Health committed mentally abnormal sex offenders - WIC § 4135:

The supervision, care, and treatment records of persons committed to the State Department of Mental Health as a mentally abnormal sex offender shall not be inspected by any person not employed by the department unless the court through an order permits examination of such records

http://www.leginfo.ca.gov/cgi-bin/waisgate?WAISdocID=39594621851+4+0+0&WAISaction=retrieve

County/state mental health prepetition screening information - WIC LPS § 5202:

Before filing a petition, the person or agency designated by the county shall request the person or agency designated by the county and approved by the State Department of Mental Health to provide pre-petition screening to determine whether there is probable cause to believe the allegations that the person is, as a result of mental disorder, a danger to others, or to himself or herself, or gravely disabled, and that the person will not voluntarily receive evaluation or crisis intervention. http://www.leginfo.ca.gov/cgi-bin/waisgate?WAISdocID=39596721890+0+0+0&WAISaction=retrieve

Information and records for services rendered by State hospitals/community mental health clinics - WIC LPS § 5328:

Information disclosed for the purpose of coordinating health care services and medical treatment, mental health services, or services for developmental disabilities, for a minor, shall not be admitted into evidence in any criminal or delinquency proceeding against the minor. However, identical evidence may be admissible in a criminal proceeding if that evidence is derived from other lawful means and is permitted by law.

http://www.leginfo.ca.gov/cgi-bin/waisgate?WAISdocID=39598721979+0+0+0&WAISaction=retrieve

Access to mental health information by participants' rights advocate - WIC LPS § 5541:

Participants' rights advocates must obtain authorization from the client or the guardian ad litem to access, copy, or use the client's confidential records and information. The client or guardian may revoke such authorization at any time http://www.leginfo.ca.gov/cgi-bin/waisgate?WAISdocID=39598721979+1+0+0&WAISaction=retrieve

Access to information related to mental health of minors -Health & Safety 123115:

A representative of a minor can be denied access to the minor's participant records where: 1) the participant records pertain to health care of a type for which the minor is lawfully authorized to consent to; or 2) the health care provider determines that granting access may have a detrimental effect on her professional relationship with the minor, the minor's physical safety or the minor's psychological well-being.

http://www.leginfo.ca.gov/cgi-bin/waisgate?WAISdocID=39636822964+0+0+0&WAISaction=retrieve

Minor consent - Health & Safety Code 123110:

Except as per 123115 and 123120, participants, minor participants authorized to consent to medical treatment, and any participant representatives shall be entitled to inspect participant records upon written request and payment of clerical costs. Such persons shall also be entitled to copies of participant records. Health care providers are prohibited from withholding participant records because of unpaid bills.

http://www.leginfo.ca.gov/cgi-bin/waisgate?WAISdocID=39636822964+0+0+0&WAISaction=retrieve

Minor's consent for medical or dental care - Family Code § 6922(a):

A minor may consent to the minor's medical care or dental care if the minor is 15 years of age or older, the minor is living separate and apart from the minor's parents, the minor is managing the minor's own financial affairs. A physician and surgeon or dentist may advise the minor's parent of the treatment given or needed if they have reason to know the whereabouts of the parent.

http://www.leginfo.ca.gov/cgi-bin/waisgate?WAISdocID=39650123406+1+0+0&WAISaction=retrieve

Minor consent for care to prevent or treat pregnancy, except sterilization - Family Code § 6925:

A minor may consent to medical care related to the prevention or treatment of pregnancy. However, a minor cannot be sterilized without the consent of the minor's parent or guardian, or except under certain circumstances, receive an abortion without the consent of a parent or guardian.

http://www.leginfo.ca.gov/cgi-bin/waisgate?WAISdocID=39650123406+1+0+0&WAISaction=retrieve

A minor who is 12 years of age or older may consent to mental health treatment or counseling on an outparticipant basis, or to residential shelter services – Family Code § 6924:

The mental health treatment or counseling of a minor authorized by this law shall include involvement of the minor's parent or guardian unless, in the opinion of the professional person who is treating or counseling the minor, the involvement would be inappropriate. The professional person shall state in the client record whether and when the person attempted to contact the minor's parent or guardian, and whether the attempt to contact was successful or unsuccessful, or the reason why it would be inappropriate to contact the minor's parent or guardian.

http://www.leginfo.ca.gov/cgi-bin/waisgate?WAISdocID=39650123406+1+0+0&WAISaction=retrieve

Minor's consent for medical treatment related to rape - Family Code 6927:

A minor who is 12 years of age or older and who is alleged to have been raped may consent to medical care related to the diagnosis or treatment of the condition and the collection of medical evidence with regard to the alleged rape. http://www.leginfo.ca.gov/cgi-bin/waisgate?WAISdocID=39650123406+1+0+0&WAISaction=retrieve

Consent for diagnosis and treatment by minor's with drug or alcohol-related problems - Family Code §6929:

When a parent or legal guardian has sought the medical care and counseling for a drug- or alcohol-related problem of a minor child, the physician shall disclose medical information concerning the care to the minor's parent or legal guardian upon his or her request, even if the minor child does not consent to disclosure, without liability for the disclosure. http://www.leginfo.ca.gov/cgi-bin/waisgate?WAISdocID=70236612795+2+0+0&WAISaction=retrieve

Minor's consent for HIV test – Health and Safety Code § 121020:

When the subject of an HIV test is not competent to give consent for the test to be performed, written consent for the test may be obtained from the subject's parents, guardians, conservators, or other person lawfully authorized to make health care decisions for the subject. For purposes of this paragraph, a minor shall be deemed not competent to give consent if he or she is under 12 years of age.

http://www.leginfo.ca.gov/cgi-bin/waisgate?WAISdocID=39661023689+2+0+0&WAISaction=retrieve

Victims of child physical abuse or neglect - Penal Code § 11171:

A physician and surgeon or dentist or their agents by their direction may take skeletal X-rays of the child with the consent of the child's parents or guardian for the purposes of diagnosing the case as one of possible child abuse or neglect and to determine the extent of the abuse or neglect. Neither psychotherapist-participant nor physician-participant privilege applies to the information reported in any court proceeding or administrative hearing.

http://www.leginfo.ca.gov/cgi-bin/waisgate?WAISdocID=39663023736+1+0+0&WAISaction=retrieve

Authorization of access to information regarding persons with disabilities to protection and advocacy agencies. – WIC 4903:

The protection and advocacy agency shall have access to the medical and other records of the following persons with disabilities: 1) any person who is a client of or requested assistance from the agency if the agency has received authorization for such access from the person or person's designated agent or other legal representative, although the person may subsequently deny such access; 2) any person that cannot be located and who is unable to authorize access due to mental or physical condition, who does not have a legal representative, and the agency has received a complaint. http://www.leginfo.ca.gov/cgi-bin/waisgate?WAISdocID=39665323781+5+0+0&WAISaction=retrieve

Persons with disabilities - Confidential information and records; disclosure; consent - WIC § 4514:

All information and records acquired in the course of providing intake, assessment, and services to persons with developmental disabilities shall be confidential. Information and records are to be disclosed only as provided in this section http://www.leginfo.ca.gov/cgi-bin/waisgate?WAISdocID=39668123833+0+0+0&WAISaction=retrieve

Local public social services agencies providing services to older persons may share information for coordination of multidisciplinary team activities – WIC § 9401:

Agencies providing services to older adults through a multidisciplinary team may provide information about older adult clients only to other county agency multidisciplinary team members providing services to same individuals to coordinate treatment between agencies. The county participants' rights advocate shall report any negative consequences of the implementation of this exception to confidentiality requirements to the local mental health director.

http://www.leginfo.ca.gov/cgi-bin/waisgate?WAISdocID=39670223885+1+0+0&WAISaction=retrieve

Papers and records pertaining to artificial insemination are subject to inspection only upon an order of the court for good cause shown – Family Code 7613:

Where a wife is inseminated artificially with semen donated by a man other than her husband, the physician and surgeon must retain the husband's consent form as part of the medical record. The record must be kept confidential and in a sealed file. However, the physician and surgeon's failure to do so does not affect the father and child relationship. All papers and records pertaining to the insemination, whether part of the permanent record of a court or of a file held by the supervising physician and surgeon or elsewhere, are subject to inspection only through a court order.

http://www.leginfo.ca.gov/cgi-bin/waisgate?WAISdocID=39672624076+1+0+0&WAISaction=retrieve

Use, disclosure and access controls for birth defects monitoring program and its contractors, researchers – Health & Safety Code § 103850:

Birth defects data created pursuant to the Birth Defect Monitoring Program must be kept confidential. All information collected for birth defects monitoring program shall be confidential and used only for the purposes stated. Access to such confidential information shall be limited to authorized program staff and persons with valid scientific interest who agree in writing to maintain confidentiality

http://www.leginfo.ca.gov/cgi-bin/waisgate?WAISdocID=39674624173+0+0+0&WAISaction=retrieve

Use, disclosure, and consent to disclose information related to hereditary diseases/congenital defects – Health & Safety Code § 124980:

All testing results and personal information generated from hereditary disorders programs shall be made available to an individual over 18 years of age, or to the individual's parent or guardian (subsection (i); all testing results and personal information from hereditary disorders programs obtained from any individual shall be confidential except for information that the individual/parent/guardian consents to be released, provided that the individual is fully informed of the scope of the information requested, the risks/benefits/purposes for the release, and the identity of to whom the inform http://www.leginfo.ca.gov/cgi-bin/waisgate?WAISdocID=39676524218+0+0+0&WAISaction=retrieve

Resources taken from: http://ohii.ca.gov/privacy360/PrivacyLaws/FederalPrivacyLaws.aspx

Federal

HIPAA Privacy Rules:

The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. The Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without participant authorization. The Rule also gives participants' rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.

http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/index.html

HIPAA Security Rules:

The HIPAA Security Rule establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information. http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/index.html

42 CFR Part 2 - Confidentiality of Alcohol and Drug Abuse Participant Records:

42 CFR Part 2 applies to AOD programs that are federally conducted, regulated or assisted in any way, directly or indirectly. Regulations apply to recipients of AOD and their participant identifiable information and prohibit most disclosures of information without participant consent.

http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&tpl=/ecfrbrowse/Title42/42cfr2_main_02.tpl

Genetic Information Nondiscrimination Act (GINA):

Under Title II of GINA, it is illegal to discriminate against employees or applicants because of genetic information. Title II of GINA prohibits the use of genetic information in making employment decisions, restricts employers and other entities covered by Title II (employment agencies, labor organizations and joint labor-management training and apprenticeship programs - referred to as "covered entities") from requesting, requiring or purchasing genetic information, and strictly limits the disclosure of genetic information.

http://www.gpo.gov/fdsys/pkg/PLAW-110publ233/html/PLAW-110publ233.htm