HIPAA PRIVACY COMPLIANCE POLICIES AND PROCEDURES

For more information, contact:

Doug Boeckmann, Privacy Officer
AXIS
2345 Rice St. Suite 112
Roseville, MN 55113
(651) 357-1109

TABLE OF CONTENTS

SECTION 1: GLOSSARY OF TERMS

HIPAA. HIPAA is the Health Insurance Portability and Accountability Act, a federal patient privacy law.

Company. Company means AXIS.

Data Practices Act. The Minnesota Government Data Practices Act is the state privacy law protecting the privacy of client information.

Individual. Individual means a person who receives services from AXIS.

Private Data is the term used under state law to describe client information that is protected under state law.

Protected Health Information (PHI) or **ePHI (electronic Protected Health Information)** are terms used under federal law to describe client information that is protected under federal law.

SECTION 2: POLICIES AND PROCEDURES

1.0 GENERAL PRIVACY COMPLIANCE POLICY AND CONFIDENTIALITY OF PRIVATE INFORMATION/PHI

All employees must be familiar with and comply with the federal HIPAA privacy regulations and the State Data Practices Act. The HIPAA privacy regulations impose a uniform, national policy on the confidentiality of patient and client records, and impose penalties for failure to comply. These federal standards are in addition to state privacy standards. The federal regulations are enforced by the Secretary of Health and Human Services (HHS) Office of Civil Rights. The state regulations are enforced by the Minnesota Department of Administration and the Minnesota Department of Human Services.

1.1 Confidentiality Policy: Information concerning Individuals served by AXIS is confidential. This means that information about specific people who receive services may not be released to anyone except:

a. the Individual or the Individual's legal representative (unless medically contraindicated before the request is made); or

b. the Individual or their legal representative has signed a valid, current Release of Information to release the information to a third party Form (Form A); or

c. there is an exception to the privacy laws that allows disclosure without a release; or

d. There is a valid and enforceable court order.

1.2 Procedure: Forward all requests for Individual consumer information to the Program Supervisor for approval. Do not release from the service location without approval for the release.

1.3 Failure to Follow Confidentiality Policy Employees who release confidential information improperly or who or fail to follow this procedure may be subject to disciplinary action up to and including termination of employment.

2.0 What is Part of the Private Data/PHI?

The Individual's Private Data/PHI includes information such as:

- progress notes;
- medication administration records;
- treatment records from other providers;
- admission information;
- discharge information;
- billing and payment records;
- treatment records;
- case management records;
- risk management plans;
- program plans;
- behavioral data records, and;
- Psychotherapy notes;

- any other records used to make decisions about the person, or;

- records from which a particular Individual can be identified, including social security number.

2.1. Other information If you are unsure whether something is part of the Private Data/PHI, contact the Privacy Officer for assistance. Do not release the information in question until you have an answer from them.

3.0 What is Not Part of the Private Data/PHI? Information not considered part of the Individual's individual record includes:

- shift change logs or "staff notebooks;"

- internal investigation information;

- employee personnel records and information;

- records from third parties, and;

- information compiled in reasonable anticipation of a civil, criminal or administration action or proceeding.

3.1. Other Information If you are unsure whether something is not part of the Private Data/PHI, contact the Privacy Officer for assistance. Do not release the information in question until you have an answer from them.

4.0 Releasing Information without a Release Form State and federal law allow certain "social responsibility" disclosures to be made without a release from the Individual. Generally, these include the following:

- reporting abuse or neglect of a child or vulnerable adult;

- disclosure for some, but not all law enforcement purposes, including grand jury proceedings;

- administrative or judicial proceedings in certain situations, but only after efforts have been made to notify the person and/or a protective order has been obtained;

- certain public health information disclosures;

- health oversight activities such as the Ombudsman for Mental Health and Mental Retardation, licensing or certification inspections;

- in response to a court order; or in response to a subpoena, but only if:

a) the party seeking the information assures AXIS that reasonable efforts have been made to get a protective order from the court preventing further disclosure of the information; or

b) the party seeking the information has been given notice of the request, and the time to object has passed, or;

c) AXIS has attempted to notify the individual to either obtain consent or give the individual the opportunity to object to the disclosure;

- certain disclosures about people who have died;

- for certain research activities;

- to avert a serious threat to health or safety;

- for specialized government functions;

- disclosures relating to organ donations;

- workers compensation disclosures;

- certain disclosures related to civil commitment proceedings, or;

- in some cases, immunization records that are released to a school.

All disclosures to other licensed caregivers or primary health care providers require an Informed Consent, except in emergency situations.

4.1. If you are unsure whether something is part of the Private Data/PHI and can be disclosed without a release, the Privacy Officer for assistance. Do not release the information in question until you have an answer from them.

5.0 Requester Identification Policy AXIS will verify the identity of a person requesting Individual information to make sure that:

1) the person has the authority to receive the information, and;

2) that the person who is requesting the records is the same person who is authorized to receive them.

Procedure: Before releasing any Individual Information, you must:

a. Request a copy of the authorization (such as a release, court order or other information appointing the person as a legal representative);

b. Ask for appropriate identification such as a driver license, state issued identification card, government issued badge or government letterhead, and;

c. Copy the verification information and put it in the individual's file.

6.0 Disclosures to Business Associates Certain people and businesses may require access to portions of the Private Data/PHI in order to do their work. AXIS must have a HIPAA Business Associate Agreement with these businesses before any information can be released to them.

Procedure:

a. give a copy of the Business Associate Agreement to anyone who receives Individual Information before you release the information, and;

b. maintain a signed copy of the agreement on a permanent basis.

7.0 Ongoing Privacy and Security Assessment Staff monitors and assesses access to Individual information on an ongoing basis. This includes:

a. Paper Records: All paper Individual records are created, maintained and stored in a physical location where other consumers or unauthorized staff or visitors may not have access to them. This includes paper records in files, at fax machines, and in printers and copiers.

b. Electronic Records: All Individual electronic records are created, maintained and stored in a way that other consumers, unauthorized staff, visitors or outsiders may not have access to them. This includes access to computers at the office or facility, at employee's homes, and on laptop computers. It may involve the use of passwords, automatic closure of files, or encryption.

Individual information is not shared by email unless the Individual has signed a consent authorizing the use of email for this purpose.

c. Verbal Communications: All verbal communication about Individuals served by AXIS is conducted in a way that other consumers, unauthorized staff, visitors or others do not overhear.

d. Understanding and Monitoring Changes in State Privacy Laws: State privacy laws may impose greater or lesser privacy protections than HIPAA. If the state and federal laws conflict, AXIS will follow the law that provides the

greater protection to the individual's privacy.

e. What to do if there is a Conflict between State and Federal Law: If there is a question about which law governs, the request will be referred to the HIPAA Privacy Officer for a response, and no information will be disclosed until the matter is decided.

8.0 Assuring Privacy - Minimum Necessary Disclosure

AXIS is charged with assuring the privacy of the Individuals it serves. Any time Private Data/PHI information is released, AXIS will release only the minimum necessary about information required to respond to the disclosure request. The "minimum necessary" rule applies both to internal uses of the information and to disclosures outside of AXIS.

Staff will carefully review any request for information including the type of information being, requested, as well as the date of the information to be disclosed, to assure that only the minimum necessary information is released.

9.0 Policies and Procedures Concerning an Individual's Access to Private Data/PHI:

9.1 Response to a Request to Inspect and Copy Private Data/PHI

Individuals have the right to inspect and copy information in their Individual Record Set. Individuals must make their request in writing. Generally, the individual are permitted to inspect and copy their record unless there is medical or program reason, as determined by a licensed professional, in advance, to deny access to all or part of the Private Data/PHI. The Individual may request a review of the decision by a second person within AXIS.

AXIS. will retain a copy of the written request in the Individual's file. AXIS may charge a reasonable fee for copying records.

AXIS will respond to a request under HIPAA to inspect and copy records within 30 days, or within 60 days if an extension is requested.

AXIS will respond to a request Under the Minnesota Government Data Practices Act within ten days.

9.2 Response to Request an Amendment to the Private Data/PHI

When AXIS receives a request from an Individual to Amend information from the Individual Record, AXIS will acknowledge receipt of the request immediately, by sending a form letter Acknowledging Receipt of Request to Amend Information.

AXIS will provide a substantive response to a client's request to Amend the Protected Data/PHI within 30 days. AXIS will either:

1) Amend the Protected Data/PHI, and send a Form Letter Granting Request to Amend, or;

2) Deny the request and provide a written explanation of why AXIS will not Amend the Protected Data/PHI and Send a Form Letter Denying Request to Amend, or;

3) Request one 30-day extension if it is not possible to comply in 30 days.

AXIS may deny access to Protected Data/PHI if the access request is reasonably likely to endanger the life or physical safety of the consumer or another person.

9.3 Response to Request for Accounting for Disclosures

AXIS documents disclosure of Individual information, and makes an accounting of these disclosures available to the Individual upon request. The accounting must cover the last six years.

AXIS will keep a record of Accountings requested and received in the Individual file.

AXIS does not provide accountings of disclosures to:

- carry out treatment, payment or health care operations;
- disclosures to the consumer, or;
- disclosures for national security or intelligence purposes.

9.4 Requests for Alternative Communication

Individuals may request that AXIS communicate with them in an alternative way or at an alternative location. For example, an Individual may ask that all communication be written rather than verbal, or that communication be sent to work rather than home.

AXIS will document these requests, and will accommodate all reasonable requests for alternative communications.

9.5 Requests for Restricted Use of Individual Information

Individuals may request that AXIS restrict use and disclosure of the individuals' records for ordinary treatment, payment or healthcare operations. For example, an Individual may ask that a particular employee, such as a AXIS employee who is a relative, not be allowed access to Individual Information. Requests will be made in writing to the Director of Program Services. AXIS will either grant or deny such a request, and document the request and the response in the Individual's record. However, if an individual has paid for a service out of their own pocket, AXIS must respect a request to restrict the use of the information.

If AXIS grants the request to Restrict Use of the Individual Information, AXIS must abide by it, except in the case of a medical emergency. An individual may not request restrictions on disclosure to him or herself, or for which a release is not required.

9.6 Request to not Release information to Health Plan

If a client has paid for a particular service in full from their own pocket, the client may ask that information about the service not be released to their Health Plan. We will honor such a request.

10.0 Privacy Notices

AXIS has a Privacy Notice that describes its policies on the use and release of Individual Information. This Privacy Notice may be amended from time to time.

AXIS will disseminate the privacy notice and any amended Notices to all Individuals receiving services. When services start, AXIS will keep proof of distribution of the notice in the Individual's file. Individuals will also sign and return consent to the use of their information and an acknowledgment of the terms of the Privacy Notice. The Privacy Notice must be re-signed whenever there is a change in the notice; the Consent must be signed at least annually, or whenever there is a change. At the time the Consent is obtained, AXIS must inform the Individual and the legal representative (if any) why the data are being collected, how AXIS intends to use the information, whether the consumer may refuse or is legally required to furnish the information, and the consequences of either providing or refusing to disclose the information. The signed notice and consents are kept in the Individual's file.

11.0 Staff Training

11.1 New Employee Orientation

AXIS trains all new employees on the HIPAA privacy standards/Data Privacy as part of their orientation procedure. This training is documented in the employee's individual training record.

11.2 Ongoing Training

After orientation, AXIS trains all employees on privacy standards on an annual basis. This training is documented in the employee's individual training record.

12.0 Privacy Officer

Doug Boeckmann is the AXIS Privacy Officer. He has the responsibility to answer questions about HIPAA privacy compliance issues and to handle employee or Individual concerns or complaints about the AXIS Individual record policies. The Privacy Officer can be reached at 651-357-1109.

13.0 Complaint and Anti-Retaliation Policy

13.1 Complaints

Individuals and employees may make complaints to AXIS about the AXIS HIPAA policies and procedures, about AXIS' compliance with its policies or procedures, or about AXIS' compliance with the HIPAA privacy regulations.

13.2 Complaint Process

Complaints may be made in person, by phone, by email, or in writing by contacting the Privacy Officer:
Doug Boeckmann
AXIS

2345 Rice St., Suite 112
Roseville, MN 55113
dcboeckmann@axis-mn.com
(651) 357-1109

Complaints may also be made directly to the government at:

Office for Civil Rights
U.S. Department of Health and Human Services
200 Independence Avenue, S.W.
Room 515F HHH Bldg.
Washington, D.C. 20201

13.3 No Retaliation
AXIS will not retaliate against an Individual or employee who makes a complaint, who participates in a HIPAA investigation or who opposes any unlawful act relating to the privacy regulations.

13.4 Complaint Records
The Privacy Officer will keep a record of all HIPAA complaints and how they are resolved, and will report to the AXIS Owners on a regular basis.

14.0 Policies and Procedures if there is a Violation of Client Privacy
A "breach" is an impermissible use or disclosure of client information that compromises the security or privacy of a client's protected health information that poses a significant risk of financial, reputational, or other harm to a client. A breach does not include an unintentional communication of client information while a staff or business associate is doing their job, or if there is a good faith belief that an unauthorized individual who received the information will not be able to retain it.

If there is a breach of privacy, the steps to be taken vary depending on how many clients are affected. The three basic tasks are to notify the individual, notify the Secretary of HHS, and in some cases, to notify the media.

An unauthorized acquisition, access, use or disclosure of client information not permitted above is presumed to be a breach unless AXIS demonstrates that there is a low probability that the client information has been compromised. In deciding this, AXIS will consider the following facts:

1. The nature and extent of the information involved, including the types of identifies and the likelihood that the information can be connected to a client;
2. The unauthorized person who used the protected health information or to whom the disclosure was made;
3. Whether the information was actually acquired or viewed, and;
4. The extent to which the risk as been mitigated.

14.1 Notice to Individuals. Individuals must always be notified of a breach.

If the number of affected clients is fewer than 10: Each individual may be contacted by first-class mail, or by telephone. If the client has agreed in advance to email notice, the individual may be contacted by email. The contact must be documented.

If the breach affects 10 or more individuals and there are 10 or more individuals for whom we do not have current contact information, the notice must be posted on the AXIS home page, or; it must be provided to a major print or broadcast media where the affected individuals likely reside.

5. The notice must be given within 60 days of the breach, and it must include all of the following:

    a. A description of the breach;

    b. A statement of the types of information involved in the breach;

    c. A description of the steps individuals should take to protect themselves from possible harm;

    d. What AXIS is doing to investigate, mitigate harm, and prevent further breaches, and;

e. Contact information concerning who to contact at AXIS for more information. If web or print media is used, there must be a toll free number for individuals to contact.

6. Notice to the Secretary of HHS. It is always necessary to notify HHS of a breach:

a. If fewer than 500 individuals are affected, the Secretary of HHS must be notified no later than 60 days after the end of the calendar year (approximately March 1) of any breaches the previous year.

b. If more than 500 individuals are affected, AXIS must notify the Secretary of HHS within 60 days of the breach. This can be done online.

7. Notifying the Media. If more than 500 individuals are affected, AXIS must also provide a press release about the breach to appropriate media outlets serving the affected area.

8. Breaches by Business Associates. If a business associate violates a client's privacy, the Business Associate is required to work with AXIS to provide the same notices that AXIS would be required to provide. Business Associates are also directly responsible for complying with the requirements of HIPAA.

All notices relating to breaches will be done in consultation with legal counsel.

15.0 Disciplinary Action Against Employees

Any employee who violates a client's privacy may be subject to disciplinary action up to and including termination of employment.

Rev. August 2013