PRIVACY AND SECURITY POLICIES

FOR

MOSAIC FAMILY HEALTH, INC.'S

HIPAA PROGRAM

AS APPROVED BY THE BOARD OF DIRECTORS ON _____, 2015

TABLE OF CONTENTS

TABLE OF CONTENTS i

TERMS, ABBREVIATIONS AND DEFINITIONS iii

PATIENTS' RIGHTS 1

AUDIO OR VISUAL RECORDINGS OF PATIENT VISITS 3

AUTHORIZATION FOR RELEASE OF PROTECTED HEALTH INFORMATION 5

BREACH NOTIFICATION 8

BUSINESS ASSOCIATE AGREEMENTS 11

PRIVACY OFFICER 13

TRAINING 14

REPORTING SUSPECTED VIOLATIONS OF PRIVACY POLICIES AND PROCEDURES 15

INVESTIGATION OF POTENTIAL PRIVACY VIOLATIONS BY A STAFF MEMBER 16

LAW ENFORCEMENT AND PUBLIC HEALTH 17

FUNDRAISING AND MARKETING 19

COMPLAINTS PROCESS 21

AMENDMENT OF HEALTH INFORMATION 24

ACCOUNTING FOR DISCLOSURES 28

TREATMENT RECORDS 31

SECURITY PERSONNEL AND SECURITY MANAGEMENT 33

CONTINGENCY PLANNING 35

SECURITY AUDIT CONTROLS AND INTERNAL AUDIT 36

WORKFORCE SECURITY TRAINING AND MANAGEMENT, WORKSTATION USE AND SECURITY 37

ACCESS CONTROL AND TRANSMISSION SECURITY 39

POLICY RETENTION, AVAILABILITY AND UPDATES..... 40

TERMS, ABBREVIATIONS AND DEFINITIONS

1.	Breach	"Breach" means the acquisition, access, use or disclosure of PHI in a manner not permitted under the regulations which compromises security or privacy of the PHI.
2.	Business Associate	"Business Associate" means a person or entity that performs certain functions or activities that involve the use or disclosure of PHI on behalf of, or provides services to, a covered entity.
3.	HIPAA	"HIPAA" stands for the Health Insurance Portability and Accountability Act of 1996, as subsequently amended.
4.	Mosaic	"Mosaic" stands for Mosaic Family Health, Inc.
5.	NPP	"NPP" stands for Notice of Privacy Practices, a description of how a covered entity may use and disclose PHI.
6.	PHI	"PHI" stands for Protected Health Information, individually-identifiable health information, as further defined by HIPAA.
7.	Psychotherapy Notes	"Psychotherapy Notes" are notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of conversation during a private counseling session or a group, joint or family counseling session and that are separated from the rest of the individual's medical record. "Psychotherapy Notes" excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests and any summary of diagnosis, functional status, the treatment plan, symptoms, prognosis or progress to date.
8.	Privacy Officer	"Privacy Officer" is the individual responsible for developing and implementing all policies and procedures required by the HIPAA privacy rules.
9.	Treatment Records	"Treatment Records" generally include registration and all other records that are created in the course of providing services to individuals for mental illness, developmental disabilities, alcoholism or drug dependence and that are maintained by treatment facilities, licensed psychologists or other licensed mental health professionals.

PATIENTS' RIGHTS

I. Policy

It is the policy of Mosaic to provide patients all the rights enumerated under HIPAA and regulations issued pursuant thereto, both as amended from time to time. Included in those rights are the right to an NPP, restrictions on confidential communications, rights to access records, rights to amend records and accountings of disclosures.

II. Description of Patients' Rights

A. Notice of Privacy Practices

As required under HIPAA, Mosaic shall provide an NPP to patients regarding the uses and disclosures that may be made regarding their PHI, and Mosaic's duties and patients' rights with respect to such notice.

1. Mosaic provides the NPP to patients on the first date of treatment. In an emergency situation, notice is provided as soon as reasonably possible.

2. Except in emergency situations, a good faith effort to obtain from a patient written acknowledgment of receipt of the NPP shall be made. If the patient refuses or is unable to acknowledge receipt of the NPP, the reason the acknowledgement was not obtained shall be documented in the patient's medical record.

3. Whenever there is a material change to uses and disclosures, patients' rights, legal duties or other pertinent sections of the NPP, Mosaic shall make available a revised NPP.

4. Mosaic makes the NPP available in the reception area and posts the NPP in the reception areas at all patient care locations. Mosaic's NPP shall be available for review on the website, mosaicfamilyhealth.org.

B. Restrictions and Confidential Communication

1. HIPAA permits patients to request restrictions on the use and disclosure of PHI for treatment, payment and health care operations, or to family members. Mosaic is not required to agree to such restrictions; however, it will attempt to accommodate a reasonable request.

2. Once Mosaic has agreed to a restriction, that restriction may not be violated; however, the restricted PHI may be provided to another health care provider in an emergency situation.

3. Patients who want to request restrictions must do so in writing.

4. Once the restriction request is received by Mosaic, the decision will be made whether the request can be honored, with the patient notified of the decision verbally or in writing, and the change documented in either the hard copy or electronic medical record.

5. If a patient wants to terminate a restriction, patient shall notify Mosaic orally or in written form of the change. Such termination will be documented in either the print or electronic medical record.

C. Accessing PHI and Requesting Medical Records

1. Patients must be permitted to request access to inspect and obtain a copy of PHI. Patients need not be permitted, however, access to inspect and obtain a copy of Psychotherapy Notes.

2. Patients have a right to make a request to have their medical record amended with respect to their PHI. (See policy on Amendment of Health Information with regard to such amendments.)

D. Accounting of Disclosures

The patient has a right to receive an accounting of disclosures upon request for disclosures made up to six years prior to the date of the request. (See policy on Accounting for Disclosures for description of the patient's rights.)

AUDIO OR VISUAL RECORDINGS OF PATIENT VISITS

I. Policy

It is the policy of Mosaic to obtain written consent from patients prior to creating any audio or visual recording of a patient visit.

II. Obtaining Consent for Recording of Patient Visit

A. From time to time, audio and/or visual recordings of patient visits may be beneficial for the education of residents at Mosaic. In those instances, Mosaic shall obtain written consent from the patient or the person legally responsible for that patient prior to creating any such recording.

B. Mosaic shall maintain a consent form for this specific purpose, which shall include the following:

1. That the audio and/or visual recording may include all aspects of the patient's visit, including, but not limited to, the interview, the physical examination and/or any diagnostic and/or treatment procedures.

2. That the patient or person acting on behalf of the patient is not required to sign the consent and that his/her decision as to whether to sign will have no bearing on care received or eligibility for benefits.

3. That the patient or person acting on behalf of the patient has the right to revoke his/her consent at any time during or after the visit.

4. That, if consent is revoked, any audio and/or visual recording will immediately stop and any audio or visual recordings already made during the visit will be permanently deleted.

5. That the recordings will not become part of the patient's medical record and will be deleted and/or destroyed once they are no longer of use as educational tools at Mosaic.

C. This consent form shall be signed by:

1. The patient, if the patient is a competent adult.

2. The patient's parent or legal guardian, if the patient is a minor.

3. The patient's legal guardian of the person, if the patient is an adult who has been adjudicated incompetent.

D. The patient or person acting on behalf of the patient shall be given a copy of the signed form.

III. Use of Recordings of Patient Visits

A. Any patient recorded for educational purposes shall not be identified in any uses of the recordings to anyone other than residents and faculty of Mosaic.

B. Any audio and/or visual recordings of a patient's visit made for educational purposes shall not become part of the patient's medical record.

C. Any audio and/or visual recordings of a patient's visit shall be deleted and/or destroyed once they are no longer of use as educational tools at Mosaic.

AUTHORIZATION FOR RELEASE OF PROTECTED HEALTH INFORMATION

I. Policy

This Policy sets forth Mosaic's process for use and disclosure of PHI pursuant to a written authorization. In accordance with the HIPAA Privacy Rules, when PHI is to be used and disclosed for purposes other than treatment, payment or health care operations, Mosaic will use and disclose it only pursuant to a valid, written authorization, unless such use or disclosure is otherwise permitted or required by law. Use or disclosure pursuant to an authorization shall be consistent with the terms of such authorization.

II. Disclosure Without Authorization

Under the HIPAA Privacy Rules, PHI may be disclosed without authorization in the following circumstances:

A. As requested by the patient or a personal representative (except in the case of Psychotherapy Notes, which need not be disclosed to the patient or patient's personal representative);

B. For purposes of treatment;

C. For purposes of Mosaic's payment activities or the payment activities of the entity receiving PHI;

D. For purposes of Mosaic's health care operations;

E. For health care operations of another covered entity, if the other covered entity has had a relationship with the patient;

F. To the Secretary of the United States Department of Health and Human Services for the purpose of determining compliance with the HIPAA Privacy Rule;

G. As required by other state or federal law (see policy on Law Enforcement and Public Health); and

H. If an individual is deceased, Mosaic may disclose PHI to a spouse, domestic partner or personal representative of the individual or, if there is no spouse or domestic partner, to an adult member of the individual's immediate family. However, the PHI disclosed must be limited to that which is relevant to the representative's representation of the estate of the deceased.

III. Use or Disclosure Pursuant to an Authorization

A. When Mosaic receives a request for disclosure of PHI, Mosaic shall determine whether an authorization is required prior to disclosing the PHI.

B. PHI may never be used or disclosed in the absence of a valid, written authorization if the use or disclosure is Psychotherapy Notes, for the purpose of marketing.

C. If for the purposes of fundraising or marketing, see Policy on Fundraising and Marketing.

D. If the use or disclosure requires a written authorization, Mosaic shall not use or disclose PHI unless the request for disclosure is accompanied by a valid authorization.

E. If the request for disclosure is not accompanied by written authorization, Mosaic shall notify the requestor that it is unable to provide the PHI requested.

F. If the request for disclosure is accompanied by written authorization, Mosaic will view the authorization to assure that it is valid.

G. Written authorization must contain the following elements in order to be honored by Mosaic:

1. In writing.

2. Name of the individual whose PHI is being disclosed.

3. Specific type of information to be disclosed. (If HIV test results are to be disclosed, this must be specified in the authorization.)

4. Name of person or entity being asked to make the disclosure.

5. Name of the individual or entity to whom the disclosure is to be made.

6. Purpose or need for the disclosure.

7. Signature of the individual or person legally authorized to give consent for the individual. If the authorization is signed by a person authorized by the individual, the relationship of the person to the individual or the basis of the person's authority to sign on behalf of the individual.

8. Date on which the consent was signed.

9. Time period during which the consent is effective.

10. Statement placing the individual on notice of the individual's right to revoke the authorization in writing, and either: 1) the exceptions to the right to revoke and how to revoke, or 2) if the right to revoke is in the notice, a reference to the notice.

11. Statement placing the individual on notice of the ability or inability to condition treatment, payment, enrollment or eligibility for benefits on the authorization.

12. Statement placing the individual on notice of the potential for information disclosed pursuant to the authorization to be subject to redisclosure by the recipient and no longer protected by HIPAA.

13. If the request is for Treatment Records, the authorization must include a statement that the individual has a right to inspect and receive a copy of the material to be disclosed.

H. If the authorization is lacking a required element, or does not otherwise satisfy the HIPAA requirements, Mosaic will notify the requester in writing of the deficiency in the authorization. No PHI will be disclosed unless or until a valid authorization is received.

I. Mosaic may not condition the provision of treatment on the receipt of an authorization except for: (i) research-related treatment; or (ii) provision of health care that is solely for the purposes of creating PHI for disclosure to a third party (i.e., performing an independent medical examination at the request of an insurer or other third party).

J. Patients may revoke their authorization at any time, provided however, the authorization may only be revoked in writing.

K. Upon receipt of the written revocation, Mosaic will write the effective date of the revocation on the authorization form.

L. Upon receipt of a written revocation, Mosaic may no longer use or disclose a patient's PHI, pursuant to the authorization. Each revocation will be filed in the patient's medical record.

M. If an individual pays an entire bill for health care services provided, the individual can request, and Mosaic must comply with a request, not to provide any information to the individual health plan regarding that treatment or procedure for which the individual paid in full.

BREACH NOTIFICATION

I. Policy

It is the policy of Mosaic to comply with the breach notification provisions established at 45 CFR 164.400. Under the regulations, "breach" means the acquisition, access, use or disclosure of PHI in a manner not permitted under the regulations which compromises security or privacy of the PHI. An impermissible use or disclosure of PHI is presumed unless and until Mosaic or the Business Associate demonstrates through its risk assessment that there is a low probability that the PHI has been compromised.

All notifications required under this Policy shall be made without unreasonable delay and in no case later than sixty (60) calendar days after discovery of a breach.

II. Guidelines

A. Breaches Do Not Include:

1. A breach does not include any unintentional acquisition, access or use of PHI by a workforce member or person acting under the authority of a covered entity or a Business Associate, if such acquisition, access or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not otherwise permitted under the law.

2. A breach also does not include any inadvertent disclosure by a person who was authorized to access PHI at Mosaic to another person authorized to access PHI at Mosaic or to an organized health care arrangement in which Mosaic participates, if the information received as a result of such disclosure is not further disclosed in a manner not permitted by law.

3. Finally, a breach does not include a disclosure of PHI where Mosaic has a good faith belief that the unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

B. Procedure

1. Any employee who discovers a suspected breach must immediately notify the Privacy Officer. The employee may notify the Privacy Officer of the occurrence of a suspected or potential breach in any format including in writing, electronically or orally. The Privacy Officer will document the report of a potential breach, along with the date and time that s/he was notified of such event.

2. The Privacy Officer will notify legal counsel of the suspected breach. If the potential breach involves PHI, legal counsel will review the matter to determine whether and how the potential breach should be reported. Legal

counsel will also determine whether any additional notifications are required pursuant to applicable breach notification law.

3. In consultation with legal counsel, the Privacy Officer will conduct an initial review of the suspected breach to determine whether a breach occurred and, if so, the scope, magnitude and severity of the breach, mechanisms for mitigating the harmful effects of the breach and ways to remediate the vulnerability that led to the breach.

4. Mosaic, in conducting its review, shall complete a four-factor risk assessment within a reasonable time after the discovery of the breach. The risk assessment shall include:

    (a) The nature and extent of the PHI involved, including the type of identifiers and likelihood of re-identification.

    (b) The identity of the unauthorized person who impermissibly used the PHI or to whom the impermissible disclosure was made. Did the recipient of the PHI have an independent obligation to protect the privacy and security of the PHI?

    (c) Was the PHI actually acquired or viewed, or was there only an opportunity to do so?

    (d) The extent to which the risk to the PHI was mitigated.

5. The above factors must be considered and documented in a risk analysis to determine whether there is a low probability that the PHI was compromised. Unless there is a low probability that the PHI was compromised, a breach notification is required.

6. If the review shows that no breach has occurred, or that there was a low probability of PHI being compromised, the Privacy Officer will document this in a report, along with all other information that supports such conclusions, and no further investigations and procedures are required.

7. If the review shows that a breach has occurred, notification will be made to the individual in accordance with the requirements of 45 CFR 164.404.

    (a) Notify each individual whose unsecured PHI has been breached within sixty (60) calendar days of discovery of the breach.

    (b) The notification shall include the following:

        (1) Date of the breach, date of discovery and a brief description of what occurred;

(2) Description of the type of unsecured PHI involved in the breach;

(3) Steps to be taken to mitigate potential harm;

(4) Description of what Mosaic is doing to investigate, mitigate and protect against future breaches; and

(5) Contact information to request information from Mosaic.

(c) The notice should be in writing by first class mail to the last known address or, if the individual agrees, electronically. In limited circumstances, an individual may opt for privacy reasons to receive communication from Mosaic orally or by telephone. In those instances, Mosaic should request the individual pick up the written notice of the breach.

8. For breaches of unsecured PHI involving fewer than 500 individuals, Mosaic shall maintain a log or other documentation of such breaches and, not later than sixty (60) days after the end of each calendar year in which the breaches were discovered, notify the Secretary of the U.S. Department of Health and Human Services.

9. If the breach involves unsecured PHI involving more than 500 individuals, Mosaic shall notify a media outlet serving in the State of Wisconsin and shall also notify the Secretary of the U.S. Department of Health and Human Services of such breach.

BUSINESS ASSOCIATE AGREEMENTS

I. Policy

It is the policy of Mosaic that for any person or entity that performs services on behalf of Mosaic, for which person or entity receives or uses PHI, a Business Associate Agreement must be obtained. A "Business Associate" is any person or organization that performs, or helps to perform, any function or activity that involves the use or disclosure of PHI on behalf of Mosaic, including, but not limited to, claims processing or administration; utilization management; benefit management; legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation or financial services; and patient safety activities. PHI may be disclosed to a Business Associate only if Mosaic receives satisfactory assurances in writing that the Business Associate will safeguard the privacy of the PHI that it creates and oversees.

II. Guidelines

A. Business Associates include subcontractors that create, receive, maintain or transmit PHI on behalf of the Business Associate.

B. Written contracts or agreements must be negotiated between Mosaic and any Business Associate that will handle PHI.

C. Business Associate Agreements shall include provisions which:

1. Identify the uses and disclosure of PHI permitted under the contract;

2. Allow the Business Associate to use or disclose the PHI only as permitted under these privacy standards;

3. Restrict use and disclosure of the PHI that the Business Associate creates or receives to those that are specified in the contract;

4. Require the Business Associate to establish safeguards to prevent use and disclosure other than as provided for in the contract with Mosaic;

5. Provide for reporting to Mosaic of any use or disclosure of PHI not provided for under the Business Associate's contract;

6. Require the Business Associate to apply the same restrictions and conditions on use and disclosure of PHI to the agents and subcontractors to whom it forwards the PHI. The Business Associate Agreement should require the Business Associate to obtain satisfactory assurance in the form of a Business Associate Agreement from its subcontractor Business Associate;

7. Make PHI available to patients as provided under patient access to health information;

8. Amend any PHI it receives when asked to do so by Mosaic;

9. Make available to Mosaic the information it needs to account for the uses and disclosures of PHI as provided for under the accounting for disclosures;

10. Require the Business Associate that is aware of non-compliance by its subcontractors to respond to the situation as Mosaic would (i.e., by trying to cure the breach, ending the violation or terminating the contract).

11. Require the Business Associate:

    (a) Where applicable, to comply with the security rule with respect to electronic PHI;

    (b) To report breaches of unsecured PHI as required by the breach notification rule;

    (c) To ensure that any subcontractor that creates, receives, maintains or transmits PHI on behalf of the Business Associate agrees to the same restrictions that apply to the Business Associate; and

    (d) To the extent that Business Associate is to carry out the covered entity's obligation under the privacy rule, to comply with the requirements of the privacy rule that apply to Mosaic in the performance of such obligation.

12. Make internal practices and its records related to the use and disclosure of PHI available to the U.S. Department of Health and Human Services for purposes of determining compliance with the privacy standards;

13. Require the return, if feasible, of PHI to Mosaic upon termination of the contract or the destruction of any copies of such information. If return or destruction of PHI is not feasible, the Business Associate must extend contractual protection for the use and disclosure of the information for purposes that make its return and destruction not feasible; and

14. Provide for termination of the contract if the Business Associate violates the contractual provisions.

[Attached to this policy is the Business Associate Agreement Template for use at Mosaic.]

PRIVACY OFFICER

I. Policy

The HIPAA regulations require designation of an individual to serve as Privacy Officer and contact person for policy development and handling of privacy inquiries and complaints. The policy of Mosaic is to comply with the HIPAA regulation by establishing the position of Privacy Officer.

II. Guidance

A. The Privacy Officer is responsible for the development and implementation of policies and procedures to safeguard the privacy of patients' health information consistent with federal and state law and regulation.

B. The responsibilities of the Privacy Officer include:

1. Developing policies and procedures;

2. Developing and conducting training programs and privacy policies and procedures;

3. Responding to questions from staff and patients concerning privacy policies and procedures;

4. Receiving complaints concerning the privacy practices described in the NPP;

5. Auditing compliance with privacy policies and procedures; and

6. Investigating and correcting violations of privacy policies and procedures.

C. The Privacy Officer may assign one or more of the above responsibilities to other staff members or contractors, but shall be responsible for making sure these responsibilities are performed.

TRAINING

I. Policy

It is the policy of Mosaic to provide appropriate training to staff on its privacy program, as well as new employees in their orientation process. The Privacy Officer shall be responsible for the development and updating of staff training programs and materials and Privacy Policies and Procedures. All staff members shall be responsible to complete privacy policy training appropriate to their job requirements.

II. Guidelines

A. The Privacy Officer or designee shall develop a privacy policy orientation and training program. The purpose of the program is to ensure that staff members are familiar with the Privacy Policies and Procedures adopted by Mosaic. The training and orientation program will cover:

1. The definition and identification of PHI;
2. Providing the NPP to all patients and obtaining a written acknowledgement of receipt;
3. Using and disclosing PHI for treatment, payment and healthcare operations only;
4. Obtaining authorization, when required, for use and disclosure of PHI;
5. Procedures for handling suspected violations of Privacy Policies and Procedures;
6. Penalties for violations of Privacy Policies and Procedures; and
7. Documentation required by the Privacy Policies and Procedures.

B. Staff members must complete the privacy policy orientation within sixty (60) days of employment at Mosaic. Completion of the privacy policy orientation and training program will be documented in the employees' personnel files by the Privacy Officer or the staff member who conducts the training.

C. Until such staff member completes the privacy policy orientation and training program, supervisors will closely monitor the use and disclosure of PHI.

D. Within sixty (60) days of employment, staff members and supervisors should confirm that the individual has completed privacy training.

E. It is the Privacy Officer's or designee's responsibility to develop training materials on new or revised Privacy Policies and Procedures.

REPORTING SUSPECTED VIOLATIONS OF PRIVACY POLICIES AND PROCEDURES

I. Policy

It is the policy of Mosaic to encourage the reporting by staff members of possible violations of Privacy Policies and Procedures to their supervisor.

II. Guidelines

A. If the supervisor determines that a violation has occurred, or that the situation warrants further investigation, possible violation should be reported to the Privacy Officer.

B. Under the following circumstances, possible violation should not be referred by a staff member to their supervisor:

1. When the violation involves the staff member's supervisor, it should be reported to the Privacy Officer; and

2. When the violation involves the Privacy Officer, it should be reported to Mosaic legal counsel.

C. Offenses that may occur include the use and disclosure of PHI that violate the practices described in the Notice of Privacy Practices and a patient's authorization.

D. Discussion of PHI in public areas should be reported if the discussion involves the disclosure of a substantial amount of PHI, and it would have been practical to conduct the discussion in a private area.

INVESTIGATION OF POTENTIAL PRIVACY VIOLATIONS BY A STAFF MEMBER

I. Policy

It is the policy of Mosaic to investigate potential violations of Privacy Policies and Procedures by a staff member.

II. Guidelines

In conducting such investigation, the Privacy Officer will:

A. Review any documents;

B. Meet with staff members or patients who reported the possible violation;

C. Meet with the staff member who may have violated the policies and procedures;

D. Determine what, if any, PHI was used or disclosed;

E. Determine whether the use or disclosure violated policies and procedures;

F. Determine whether the violation was accidental or intentional;

G. Recommend to the staff member's supervisor disciplinary action, if any, that should be taken; and

H. Document the findings of the investigations and actions taken.

LAW ENFORCEMENT AND PUBLIC HEALTH

I. Policy

Mosaic shall disclose PHI to various governmental entities as required by law. In general, disclosure to governmental entities, as mandated by the law, does not require the authorization of the patient.

II. Guidelines

A. Reporting of abuse, neglect and domestic violence. Mosaic shall report cases of suspected child abuse and neglect as required by law. Any such reports must follow the policies and procedures established. Mandatory reporting of child abuse and neglect might involve disclosure of PHI. Mandatory reporting of abuse, neglect and domestic violence might also involve disclosure of PHI. HIPAA regulations permit disclosure of PHI to government agencies responsible for investigating abuse, neglect and domestic violence, including child abuse and neglect.

B. Mosaic staff may disclose PHI requested by law enforcement agencies without obtaining the patient's authorization in the following situations:

1. Any information requested by a Subpoena, Court Order or Summons in accordance with Section III D of this Policy;

2. The name, address, date and place of birth, Social Security number, blood type and Rh factor, type of injury, date and time of treatment or death, and description of the physical characteristics of a patient when requested by a law enforcement official;

3. PHI that is evidence of criminal conduct on the premises of Mosaic; or

4. PHI concerning emergency treatment when the disclosure is necessary to alert law enforcement agencies of the commission of a crime, the location of the victim of a crime or the identity, description or location of a suspected perpetrator of a crime.

C. Mosaic may disclose PHI to a government agency, such as the U.S. Department of Health and Human Services and the Wisconsin Department of Health Services, which are responsible for administering public health programs, such as Medicare and Medicaid, and to licensing providers conducting audits and for other purposes related to the oversight of the health system.

D. Mosaic may disclose PHI for use in legal proceedings under the following circumstances:

1. The information has been requested in a Court Order, or an Order of an Administrative Tribunal; or

2. The information has been requested by means of a Subpoena, discovery request or other legal process.

E. Before responding to any under Section III D above, efforts should be made to ensure that disclosure is limited to the minimum PHI specifically requested and that the following assurances are obtained:

1. The party seeking the PHI has made a good faith effort to provide a written notice to the subject of the request and has provided sufficient information to the subject of the request to permit the individual to object to the disclosure and to resolve any objections that may have been raised; or

2. The party seeking the PHI provides written documentation that it has entered into or has otherwise obtained a qualified protective order that:

   (a) Prevents the parties to the legal action from using or disclosing PHI for any purpose not related to the litigation or legal proceeding for which the information was requested; and

   (b) Requires the return or destruction of the PHI at the conclusion of the proceeding.

F. Mosaic may provide to a school proof of immunization of a student or prospective student if the school is required by state or other laws to have such proof of immunization prior to admitting the student and Mosaic obtains and documents the agreement for disclosure from a parent, guardian or other person in place of the parent, or the student if the student is an adult or emancipated minor.

FUNDRAISING AND MARKETING

I. Policy

It is the policy of Mosaic that the use of PHI in marketing and fundraising activities must conform to the requirements contained herein. Whether the patient's authorization is required for fundraising and marketing depends on how the marketing communications and fundraising appeals are structured by Mosaic.

II. Guidelines

A. Marketing and Communications That Do Not Require Authorization

The following communications do not require authorizations:

1. Communication to members of health plans that describe Mosaic and the services that are available from Mosaic;

2. Communication to a patient as part of the patient's treatment that are specific to the medical condition of the patient;

3. Communication from the patient's health plan during treatment for the purpose of alerting the patient to the availability of alternative treatments, therapies, health care providers and treatment centers;

4. Face-to-face communication between Mosaic staff members and patients during a patient visit; and

5. Promotional gifts of nominal value, such as pens, notepads and coffee mugs.

B. Marketing Activities That Require Authorization

1. A patient must specifically authorize the use of PHI collected or maintained by Mosaic for communication that is sent to the individual describing a product or service offered by an organization other than Mosaic. If Mosaic receives "financial remuneration" for such a use or disclosure of PHI, the authorization must contain a statement notifying the patient that remuneration is involved. For purposes of this paragraph, "financial remuneration" means direct or indirect payment from or on behalf of a third party whose product or service is being described. Direct or indirect payment does not include any payment for treatment of an individual.

2. In addition, Mosaic must obtain patient authorization before sending marketing materials which are paid for by a third party. Marketing activities may include mailing by pharmaceutical companies, retail

pharmacies and suppliers of unrelated medical services, such as DME companies.

3. Mosaic's NPP shall contain a statement indicating that uses and disclosures of PHI for marketing purposes and disclosures that constitute a sale of PHI require an individual's written authorization.

4. Marketing does not include:

   (a) Communications made to provide refill reminders or otherwise communicate about a drug or biological that is currently being prescribed to an individual, if any financial remuneration received by Mosaic in exchange for making the communication is reasonably related to Mosaic's cost of making the communication;

   (b) A communication made for treatment and health care operation purposes, except where Mosaic receives payment in exchange for making the communication; or

   (c) Face-to-face communication, even if payment is received from a third party promoting health in general, that does not promote a product or services from a particular provider.

C. Fundraising Activities

1. Demographic information describing the individual (date of birth, sex, marital status, address and other non-clinical information), as well as dates on which the patient received health care services from Mosaic, may be used to support efforts to raise funds that directly benefit Mosaic without the patient's authorization.

2. PHI may not be used in any fundraising activities without authorization by the patient. The patient's authorization is required for the use of any PHI, except demographic information and dates of service.

COMPLAINTS PROCESS

I. Policy

It is the policy of Mosaic to resolve, document and mitigate complaints regarding privacy policies and procedures in accordance with the procedures established herein.

II. Guidelines

A. Submission of Complaints

A patient or other individual who wants to file a complaint concerning Mosaic's privacy policies and procedures or a suspected disclosure of PHI that violates federal or state law should be directed to the Privacy Officer for answers to questions about filing complaints.

B. Complaints Concerning Privacy Policies and Procedures

The procedures for resolution of complaints submitted by patients or other individuals concerning the privacy practices of Mosaic are outlined below.

1. Upon receiving a complaint (either a complaint form or a letter outlining a complaint), the Privacy Officer or a designated staff member will review the complaint, evaluate the specific details of the complaint and determine whether the complaint warrants a change in the privacy policies or procedures of Mosaic.

2. If a change appears to be warranted, the staff member conducting the evaluation will develop a recommendation and submit it to the Privacy Officer, who will determine whether an immediate change in policies and procedures is needed to prevent a violation of federal or state privacy standards, laws or regulations.

3. If it is determined that a change in policies and procedures is necessary, a revised policy will be prepared following the procedures outlined in Procedures for Updating Privacy Policies and Procedures. A response should be prepared by the Privacy Officer and sent to the individual submitting the complaint. The response should thank the individual for his or her interest, and it should indicate that the suggestion has been evaluated.

4. If a change does not appear to be warranted, a response to the complaint will be prepared by the Privacy Officer and sent to the individual submitting the complaint. The response should thank the individual for his or her interest. It should indicate that the suggestion has been evaluated, but that Mosaic believes that its current privacy procedures comply with federal and state requirements and are sufficient to protect patient privacy.

5. Receipt of the complaint and its final disposition should be documented using the procedures established by Documentation of Complaints, Section III D.

C. Complaints Arising from Possible Violations of Privacy Policies

The procedures for resolution of complaints submitted by patients or other individuals concerning the disclosure of PHI are outlined below.

1. A staff member who receives a complaint from a patient or other individual that concerns a possible use or disclosure of PHI that violates Mosaic's privacy policies and procedures, or that violates federal and state law, should immediately refer the complaint to the Privacy Officer.

2. The Privacy Officer will review the complaint and determine whether a violation occurred and, if so, whether the violation involves only the privacy policies and procedures established in this manual or also involves a violation of federal and state privacy laws and standards.

3. If the Privacy Officer determines the complaint may involve a violation of federal or state standards and legal requirements, s/he will immediately forward the complaint to Mosaic's legal counsel for evaluation. The request for evaluation should specify a date by which the evaluation should be completed.

4. The Privacy Officer should follow up and track the status of the referral. If the evaluation indicates that federal or state standards may have been violated, the mitigation procedures established in Mitigation, Section III E, should be followed.

5. If the Privacy Officer determines that the complaint does not involve a violation of federal or state standards and legal requirements, s/he will determine whether Mosaic's privacy policies and procedures were violated. If policies and procedures have been violated, the disciplinary procedures established by Reporting of Suspected Violations of Privacy should be initiated.

6. Upon completion of step 4, the Privacy Officer should contact the person submitting the complaint and notify him or her of the actions that will be taken to address the complaint.

7. Evaluations of complaints should generally be completed within thirty (30) days of receipt.

8. The receipt of the complaint and the final disposition should be documented using the procedures established by Documentation of Complaints, Section III D.

D. Documentation of Complaints

The Privacy Officer will establish and maintain files containing documentation of all complaints received. This documentation will include the actions taken to address or resolve the complaint, including any written correspondence with the person submitting the complaint.

E. Mitigation

When the Privacy Officer determines that a use or disclosure of PHI has violated the policies and procedures established by this manual, the case will be referred to Mosaic's legal counsel to:

1. Determine any action needed to mitigate any harm that may result to the patient whose information was used or disclosed;

2. Evaluate Mosaic's legal exposure and recommend a course of action; and

3. Follow up with the patient.

All communications with the patient concerning use or disclosure of PHI that legal counsel determines may violate federal or state standards and legal requirements should be handled by Mosaic's legal counsel.

AMENDMENT OF HEALTH INFORMATION

I. Policy

A patient may request amendment of the information maintained by Mosaic in the designated record sets listed below. The patient must follow the procedures outlined in Procedures for Requesting Amendment of Information when requesting amendment of information maintained by Mosaic.

II. Guidelines

A. Designated Record Sets

A patient may request amendments to information contained only in the following record sets:

1. The patient's medical records;

2. The patient's billing records; and

3. Other records that contain PHI used to direct treatment.

B. Procedures for Patient Request for Amendment

1. The patient must request amendment of PHI.

2. The request will be reviewed as provided for in Action on Requests for Amendment of Information, Section III C.

3. If the request is approved, the PHI will be amended as provided for in Procedures for Amendment of Records (Section III E), Procedures for Amendment of Internal Records (Section III F) and Notifying Other Parties That Information Has Been Amended (Section III G),.

4. If the request is denied, the patient will be notified and offered the opportunity to describe the reasons for his disagreement in writing. The patient's statement will then be handled using the procedures in Denial of Request for Amendment (Section III H), Statement of Disagreement (Section III I) and Rebuttal of Disagreement (Section III J).

C. Action on Requests for Amendment of Information

The Privacy Officer may deny a patient's request to amend records if the following criteria are met:

1. The information to be amended was not created by Mosaic, but was received from another entity;

2. The information to be amended is accurate and complete;

3. The information to be amended does not exist in the specified records; and

4. The information to be amended is not available for inspection by the patient or the patient's representative.

Action must be completed on any request for amendment within sixty (60) days of receiving the request. If action cannot be completed within sixty (60) days, Mosaic must notify the patient of the delay, including the reasons for the delay, and complete the review within ninety (90) days of the date the request was originally received.

D. Procedures for Review of and Response to Patient Request

1. Patient information amendment requests should be forwarded to the Privacy Officer.

2. The Privacy Officer should contact the patient's physician, or a staff member s/he designates, and request a review of the requested amendments.

3. The physician or designated staff member should indicate which of the requested amendments should not be made because the information in the patient's record is accurate and complete or meets the other requirements for denying a request that are listed above.

4. The physician or designated staff member should then return the form to the Privacy Officer.

5. The Privacy Officer should review the form after it is returned by the patient's physician and identify any information that should be amended.

6. The Privacy Officer should initiate the procedures for amending PHI specified by policies Procedures for Amendment of Records (Section III E), Procedures for Amendment of Internal Records (Section III F) and Notifying Other Parties That Information Has Been Amended (Section III G).

7. The Privacy Officer should prepare a response to the patient as required by Denial of Request for Amendment (Section III H), Statement of Disagreement (Section III I) and Rebuttal of Disagreement (Section III J), as applicable.

E. Procedures for Amendment of Records

When a request to amend patient information is approved, the Privacy Officer will:

1. Initiate the procedures established by Procedures for Amendment of Internal Records (Section III F) to update the records maintained by Mosaic; and

2. Initiate the procedures established by Notifying Other Parties That Information Has Been Amended (Section III G) to explain the amendment to other parties to whom the information had previously been disclosed.

F. Procedures for Amendment of Internal Records

1. When a patient's request for amendment of PHI is approved, either of the following procedures should be followed:

   (a) The records containing the affected information should be updated; or

   (b) The amended information should be linked to the original information.

2. The Privacy Officer will refer the request for amendment to the Mosaic staff member responsible for maintaining the affected records.

3. That staff member will identify the records that need to be amended.

4. Those records should either be amended or should be linked to the amended information (that is, contained in a new or corrected record where it will be available when the affected information is used or disclosed in the future).

G. Notifying Other Parties That Information Has Been Amended

When a patient's PHI is amended in response to a request received from the patient, other organizations to which the PHI being amended has been disclosed will be notified of the amendment. Organizations to be notified include:

1. Business Associates, health plans and other providers the Privacy Officer can identify as having received the PHI; and

2. Persons and organizations the patient can identify as having received the PHI that requires amendment, but only to the extent that the Privacy Officer can confirm that these persons or organizations previously received the PHI.

Mosaic is not required to confirm that the organizations or other entities notified of the amendment have updated their records.

H. Denial of Request for Amendment

When a request to amend PHI is denied, the patient will be informed in writing of the decision. The notice sent to the patient must advise the patient of the following:

1. The patient may submit a statement of disagreement that will become part of his or her records and will, in the future, be disclosed to any person or organization that receives the identified PHI.

2. If the patient does not submit a statement of disagreement, s/he may ask Mosaic to include the request for amendment and the denial in any future disclosure of the identified PHI to any person or organization that receives the identified PHI.

3. The patient may file a complaint with the provider concerning the request for amendment (a description of how the patient can file this complaint must be included in the privacy notice).

4. The letter must identify the name, mailing address and telephone number of the Privacy Officer.

I. Statement of Disagreement

If the patient disagrees in writing when notified that a request for amendment of PHI has been denied, the Privacy Officer will review it and will append it to or otherwise or link it to the patient's record. This will ensure that it will accompany the original information when it is used or disclosed in the future.

The Privacy Officer may prepare an accurate summary of the patient's Statement of Disagreement if s/he believes that a summary will adequately provide a clear understanding of the disputed information.

J. Rebuttal of Disagreement

If a patient disagrees in writing when notified that a request for amendment of PHI has been denied, the Privacy Officer will review the statement and determine whether a formal rebuttal or response, as provided for in federal regulations, is necessary. If it is determined that a rebuttal is necessary, the Privacy Officer will prepare and append it to the patient's records.

1. The Privacy Officer will consult as necessary with the patient's physician or other staff members to make this determination.

2. Both the patient's Statement of Disagreement and the rebuttal statement will be noted in the patient's records.

3. The Statement of Disagreement and the rebuttal either will be included in the patient's records, or will be linked to those records to permit them to be included with the original information when it is used or disclosed in the future.

4. A copy of the rebuttal statement will be sent to the patient.

ACCOUNTING FOR DISCLOSURES

I. Policy

The procedures below establish the process of Mosaic to follow related to providing patients with an accounting of disclosures of PHI.

II. Guidelines

A. Maintenance of Records of Disclosures

The Privacy Officer will create a system for documenting all disclosures of PHI for which an individual may request an accounting. Disclosures of PHI that Mosaic is not required to report to a patient include:

1. Any disclosure for the purpose of treatment, payment or the day-to-day operations of Mosaic that is a disclosure of information permitted under the notice;

2. Any disclosure specifically authorized by the individual;

3. Any disclosure to the patient himself or herself;

4. Any disclosure for use in a facility directory;

5. Any disclosure to national security or intelligence agencies required by law;

6. Any disclosure to correctional institutions or law enforcement agencies required by law;

7. Any disclosure that is part of a limited data set; and

8. Any disclosure that occurred prior to April 14, 2003 (the effective date of the HIPAA Privacy Rule).

B. Accounting to Patients for Disclosures of Information

To receive an accounting of disclosures of PHI, a patient must submit a written request to the Privacy Officer.

1. A patient who indicates to any Mosaic staff member that s/he would like to receive an accounting of disclosures should be told to contact the Privacy Officer.

2. The Privacy Officer will provide the patient with a disclosure accounting form and review the types of disclosures that will be reported in the accounting.

3. The Privacy Officer will determine whether the ability of the patient to obtain an accounting of disclosures has been suspended in response to a request from a law enforcement or health oversight agency.

4. If the patient's right to an accounting has not been suspended, the Privacy Officer will initiate the preparation of an accounting as provided for by Information to Be Provided in an Accounting of Disclosures.

C. Charges for Accountings of Disclosures

If a patient requests more than one accounting during any twelve (12) month period:

1. The patient will not be charged for the first accounting; and

2. If the patient received an accounting for which s/he was not charged during the preceding twelve (12) months, s/he will be informed that Mosaic will charge $20.00 for the second accounting. If the patient agrees to pay this fee, the accounting will be provided.

D. Suspension of a Patient's Right to Receive an Accounting of Disclosures

1. A law enforcement or health oversight agency may request the provider to suspend the right of an individual to request an accounting of disclosures.

2. Requests from law enforcement agencies should be submitted in writing. The written statement should indicate that providing an accounting is likely to impede the agency's activities and should specify a time period during which the patient's right will be suspended.

3. Suspensions that last more than thirty (30) days must be supported in writing. Requests must be made in writing. If a written request is not submitted, the individual's right to an accounting may be suspended for no more than thirty (30) days.

4. A communication from a law enforcement or health oversight agency requesting the suspension of a patient's right to an accounting of disclosures should be directed to the Privacy Officer.

5. The Privacy Officer will verify the credentials of the government official that makes a verbal request and document the identity of the official or agency.

6. The Privacy Officer will place the patient's name on a list of persons whose right to an accounting has been suspended pursuant to an official request.

E. Information to Be Provided in an Accounting of Disclosures

The information that will be provided in an accounting of disclosures includes:

1. The date of the disclosure;

2. The name of the entity or person who received the PHI; and

3. A brief description of the purpose of the disclosure or a copy of the authorization for the disclosure.

Note: Disclosures to Business Associates for purposes of treatment, payment and health care operations should not be included in the accounting.

F. Documentation of Accountings Provided to Patients

Copies should be made of all accountings of disclosed information prepared for patients. The copies should be kept for six (6) years.

G. Documentation of Disclosures Requiring an Accounting

1. When a staff member discloses PHI, the disclosure will be documented by that staff member. This documentation would be needed to produce an accounting of disclosures if the patient were later to request an accounting.

2. Any disclosure, other than a disclosure for purposes of treatment, payment or health care operations, will be documented by completing a disclosure accounting form.

3. The disclosure accounting form will be forwarded to the Privacy Officer, who will update the files and databases that are used to prepare accountings of disclosures.

TREATMENT RECORDS

I. Policy

The procedures below establish the additional policies of Mosaic to follow related to the use and disclosure of Treatment Records. Except as otherwise set forth below, Treatment Records shall be subject to the same general policies and procedures that relate to other medical records kept by Mosaic.

II. Guidelines

A. Notice Describing Treatment Records Access Procedures

Mosaic shall prominently display a notice describing Mosaic's Treatment Record access procedures and shall make this notice available for inspection and copying upon request.

B. Uses and Disclosures in General

1. No PHI contained in Treatment Records will be released by Mosaic to a person previously unknown to Mosaic unless there is reasonable assurance regarding the person's identity.

2. Mosaic shall not acknowledge whether an individual has applied for, has received or is receiving services for mental illness, developmental disabilities, alcoholism or drug dependence, except with the informed consent of the individual or as otherwise required by law. All inquiries regarding whether a person is or was receiving such services and that do not fit within one of the accepted disclosures without authorization set forth below shall be responded to by stating: "It is Mosaic's policy not to provide that information," or words to that effect. All Mosaic staff who normally deal with patient status inquiries shall be trained in this procedure.

C. Disclosure Without Authorization

Under the HIPAA Privacy Rules and Wisconsin law, Treatment Records may be disclosed without authorization only in limited circumstances, including the following:

1. Treatment Records may be made available to treatment staff within Mosaic when and to the extent that performance of their duties requires that they have access to such information.

2. Treatment Records may be released to a physician or his or her designee for treatment of the individual in a medical emergency, if the physician is otherwise unable to obtain the individual's informed consent because of the individual's condition or the nature of the emergency. Disclosure in this situation shall be limited to that part of the records necessary to meet the medical emergency.

3. Certain information from Treatment Records may be disclosed to a health care provider, or to any person acting under the supervision of the health care provider, who is involved with the individual's care, if necessary for the current treatment of the individual. Information that may be released under these circumstances is limited to:

   (a) The individual's name, address and date of birth;

   (b) The name of the individual's provider of treatment services;

   (c) The date of any of those treatment services provided;

   (d) The individual's medications, allergies, diagnoses, diagnostic test results and symptoms; and

   (e) Other relevant demographic information necessary for the current treatment of the individual.

4. Should Mosaic receive a request for the unauthorized disclosure of Treatment Records under any circumstances not set forth immediately above, Mosaic will consult with its legal counsel.

D. Use or Disclosure Pursuant to an Authorization

1. If Mosaic is the recipient of Treatment Records, it shall not re-release any PHI contained in said Treatment Records unless re-release is specifically authorized by informed consent of the individual or as otherwise required by law.

2. Mosaic shall accompany any disclosure or re-release of PHI in Treatment Records, other than oral disclosures, with a written statement which states that the PHI is confidential and disclosure without patient consent or statutory authorization is prohibited by law.

3. Treatment Records may be released to third-party payers only with informed consent.

SECURITY PERSONNEL AND SECURITY MANAGEMENT

I. Policy

Mosaic, in an effort to be compliant with the HIPAA Security Rule, has designated a Security Officer to oversee Mosaic's maintenance of reasonable and appropriate administrative, technical and physical safeguards for safeguarding the confidentiality, integrity and availability of PHI and Mosaic information systems.

II. Guidelines

A. Position of Security Officer

Mosaic shall assign responsibility for protecting the confidentiality, integrity and availability of Mosaic information systems and PHI to a Security Officer. This position will be responsible, in collaboration with the Privacy Officer and other Mosaic workforce as appropriate, for developing, implementing and monitoring policies and procedures necessary to appropriately protect PHI and the information systems in which it is stored or transmitted. Such policies and procedures will control the conduct of the workforce, subcontractors and Business Associates with regard to the protection of PHI.

The Security Officer will also coordinate the selection, implementation and administration of security controls, organize security training and conduct periodic evaluations of the Mosaic information systems. In this manner, Mosaic will prevent unauthorized access to its information systems and PHI, while providing necessary and appropriate access to properly-trained workforce members.

B. Response to Security Incidents

The Security Officer, in response to any suspected or known security incidents, will mitigate, to the extent practicable, any harmful effects and work with the Privacy Officer as necessary to analyze and document the security incident and its outcome in accordance with Mosaic's Breach Notification policy.

C. Risk Analysis

In order to identify and mitigate risks inherent in Mosaic's information systems, the Security Officer will conduct an annual assessment of all identified servers and databases that contain PHI to identify and prioritize potential risks and vulnerabilities to the confidentiality, integrity and availability of electronic PHI and information systems.

D. Risk Management

Risks identified during the annual assessment will be monitored and managed on an on-going basis and minimized to a level deemed reasonable and appropriate by Mosaic management and the Security Officer.

The Security Officer will also perform and/or direct both a technical and nontechnical evaluation of Mosaic security policies and procedures on at least an annual basis to evaluate whether they are effective and appropriate, to identify any discrepancies between such policies and procedures and actual practices, and to assess how well its security policies and procedures meet the requirements of the Security Rule, taking into account environmental or operational changes affecting the security of PHI.

E. Implementation of Security Measures

Selection and implementation of security measures to reduce risk to information systems will be based on Mosaic's review of risk assessments, security incidents and ongoing monitoring.

CONTINGENCY PLANNING

I. Policy

Mosaic, in an effort to be compliant with the HIPAA Security Rule, sets out in this policy the requirements for safeguarding PHI through contingency planning.

II. Guidelines

Mosaic will maintain and implement Contingency Plan policies and procedures. Mosaic will test and revise these plans as necessary to assure that they function as planned and that they are effective.

A. Data Backup Plan

It will be Mosaic's policy to assure, by means of a Data Backup Plan that Mosaic has adequate backup of electronic PHI. Backup and restore procedures will be updated regularly and will ensure Mosaic creates and maintains retrievable exact copies of electronic PHI. In addition, Mosaic will assure that the backup data can be accessed quickly.

B. Disaster Recovery Plan

Mosaic will maintain a Disaster Recovery Plan to restore any loss of data. This plan which will cover the full range of information and activities needed to assure that the plan will function smoothly in situations where it is needed.

C. Emergency Mode Operation Plan

Mosaic will maintain an Emergency Mode Operation Plan that will enable continuation of critical business processes for the protection of the security of electronic PHI while operating in emergency mode.

SECURITY AUDIT CONTROLS AND INTERNAL AUDIT

I. Policy

Mosaic, in an effort to be compliant with the HIPAA Security Rule, sets out in this policy the requirements for safeguarding PHI through audit controls and internal auditing.

II. Guidelines

A. Information System Activity Review

Mosaic will establish and maintain ongoing processes to review records of systems activity, such as log-ins, file accesses and security incidents, for PHI. The Security Officer will establish documented procedures for auditing this information for the purpose of identifying security breaches and for assuring that users comply with access controls. The Security Officer will assign specific individuals or job functions that will be responsible for such internal audit activity. Any unusual or irregular activity will be promptly investigated.

B. Audit Controls

Mosaic will implement hardware, software and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic PHI.

C. Person or Entity Authentication

Mosaic will implement procedures to verify that a person or entity seeking access to electronic PHI is the one claimed.

D. Access to Audit Logs

Access to audit logs will be limited to those assigned to the internal audit and control function as described above.

WORKFORCE SECURITY TRAINING AND MANAGEMENT, WORKSTATION USE AND SECURITY

I. Policy

Mosaic, in an effort to comply with the HIPAA Security Rule, sets out the following policy, recognizing that Mosaic's workforce is the foundation for its security environment.

II. Guidelines

Mosaic will create and maintain procedures directed toward the behavior of its workforce that promote an environment for PHI that is reasonably secure from accidental, intentional or inadvertent disclosures. Mosaic will authorize access to PHI only to the extent appropriate based on the user or recipient's role. Mosaic will implement physical safeguards for all workstations that access PHI to restrict access to authorized users.

A. Workstation Use and Security

Mosaic will develop and maintain written guidelines on workstation use, which will address:

1. The proper functions to be performed;

2. The manner in which those functions are to be performed – the documentation of the actual function and how it is to be performed; and

3. The attributes of the physical environment in which the workstations, including laptops and other portable devices, are to be located. The attributes will vary based on the sensitivity of information that typically is accessed from that environment. Attributes include such things as physical access to the workstation itself and to the area it is located in, and removable media such as USB flash memory and CD-ROMs, and best practices concerning password management.

The Security Officer will oversee this process and assure that the workforce is trained on these guidelines prior to being given access to the system. Physical safeguards will be implemented for all workstations that access electronic PHI to restrict access to authorized users.

B. Security Awareness and Training

Security awareness training will be provided to all members of the Mosaic workforce, including management. Awareness training will be directed at all of these individuals, regardless of their roles or access to PHI. The purpose of the training will be to provide education around such things as password maintenance, security incident reporting, and virus and other forms of destructive software. The Security Officer will oversee the development of awareness training.

It will also be Mosaic's policy to provide training to all users of electronic systems. User training will be required prior to any user receiving access to the system. User training will

focus specifically on the actual usage of security features such as virus protection practices, addition of unauthorized hardware or software to the system, password management, login practices, automatic logoffs, etc. The Security Officer will oversee the development of awareness training in conjunction with Human Resources.

C. Device and Media Controls

Mosaic will implement procedures for device and media controls, removal of PHI from electronic media before it is available for re-use, and the final disposition of electronic PHI and the hardware or electronic media on which it is stored.

Installation and assignment of hardware and software within Mosaic's information systems that contain PHI will be subject to management approval in consultation with the Security Officer.

Mosaic will maintain records of ownership, assignments and movement of hardware and mobile media and ensure that only authorized individuals may access them.

D. Sanction Policy

Mosaic workforce members will not be permitted to use information systems for the storage or transmission of PHI that have not been approved by the Security Officer and Mosaic management.

Mosaic workforce members will be trained not to provide access to Mosaic informational systems to unauthorized persons and not to attempt to gain access to information systems or PHI except to accomplish their legitimate job responsibilities.

Mosaic will apply appropriate sanctions, which may include disciplinary action up to and including termination, against workforce members who fail to comply with Mosaic's HIPAA policies and procedures regarding the safeguarding and security of PHI.

E. Termination Procedures

Mosaic will establish procedures for terminated workforce members and for members of the workforce whose positions and work assignments have changed. These procedures will cover security for PHI in all media. These procedures will address:

1. Physical access to PHI;

2. Removal of access privileges, both general access and user levels of access; and

3. The collection of keys or other objects that allow access.

ACCESS CONTROL AND TRANSMISSION SECURITY

I. Policy

Mosaic, in an effort to be compliant with the HIPAA Security Rule, sets out in this policy the requirements for safeguarding PHI by controlling access to its facilities and information systems.

II. Guidelines

A. Physical Access to Hardware and Paper Records

Mosaic will create and maintain procedures to safeguard all of its locations from unauthorized physical access and to safeguard hardware and other equipment from unauthorized physical access, theft and interference.

Mosaic will limit and control physical access to any and all parts of the designated record set. Mosaic's paper medical record files will be placed in limited access spaces, and access to those records will be controlled by appropriate staff.

B. Access to Electronic Files

Electronic files will be subject to access controls that will limit user access to that PHI for which they have clearance. Controls for access to non-PHI data will be established and maintained in accordance with context-, role-, or user-based criteria.

These controls will include a process for setting criteria for granting access and for modification of the criteria. With regard to access of electronic PHI, Mosaic will establish user-based access and audit controls that will assign a unique name and/or number for identifying and tracking user identity, and define users, data sources, data accessed, the client, the date and time of the access and other information it considers appropriate. Mosaic will establish electronic processes as appropriate that terminate sessions of access to PHI after a predetermined time of inactivity. Mosaic will also establish (and implement as needed) procedures for obtaining necessary PHI during an emergency.

POLICY RETENTION, AVAILABILITY AND UPDATES

I. Policy

Mosaic, in an effort to be compliant with the HIPAA Security Rule, sets out in this policy the requirements for retaining these Policies, making them available to the appropriate persons and updating them as needed.

II. Guidelines

A. Retention

Mosaic shall retain a copy of these Policies for six (6) years from the date of their creation or the date when they last were in effect, whichever is later.

B. Availability

Mosaic shall make these Policies available to those persons responsible for implementing the policies and procedures described herein.

C. Updates

Mosaic shall review these Policies periodically and update them as needed, in response to environmental or operational changes affecting the security of electronic PHI.