# Table of Contents

## Privacy Policies

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>5</td>
</tr>
<tr>
<td>Definitions</td>
<td>6</td>
</tr>
<tr>
<td>Personal Representatives</td>
<td>13</td>
</tr>
<tr>
<td>Active Directory</td>
<td>17</td>
</tr>
<tr>
<td>Verification of Identity</td>
<td>18</td>
</tr>
<tr>
<td>Notice of Privacy Practices</td>
<td>20</td>
</tr>
<tr>
<td>Patient Access to Protected Health Information</td>
<td>22</td>
</tr>
<tr>
<td>Accounting of Disclosures</td>
<td>26</td>
</tr>
<tr>
<td>Communication by Alternative Means</td>
<td>29</td>
</tr>
<tr>
<td>Right to Amend Records</td>
<td>31</td>
</tr>
<tr>
<td>Right to Request Restriction on Use and Disclosures</td>
<td>34</td>
</tr>
<tr>
<td>HIPAA Compliance Officer Designation</td>
<td>36</td>
</tr>
<tr>
<td>Privacy Complaint Reporting and Tracking</td>
<td>37</td>
</tr>
<tr>
<td>Documentation</td>
<td>38</td>
</tr>
<tr>
<td>Retaliation and Intimidation</td>
<td>39</td>
</tr>
<tr>
<td>Mitigation</td>
<td>41</td>
</tr>
<tr>
<td>Amendment of Privacy Practices and Policies</td>
<td>42</td>
</tr>
<tr>
<td>Waiver of Rights</td>
<td>44</td>
</tr>
<tr>
<td>HIPAA Compliance Training</td>
<td>45</td>
</tr>
<tr>
<td>Safeguards</td>
<td>47</td>
</tr>
<tr>
<td>Sanctions</td>
<td>53</td>
</tr>
<tr>
<td>Uses and Disclosures</td>
<td>55</td>
</tr>
<tr>
<td>Minimum Necessary Rule</td>
<td>57</td>
</tr>
<tr>
<td>Treatment, Payment, and Health Care Operations</td>
<td>60</td>
</tr>
<tr>
<td>Authorization</td>
<td>62</td>
</tr>
<tr>
<td>Mental Health Records and Psychotherapy Notes</td>
<td>64</td>
</tr>
<tr>
<td>Required by Law</td>
<td>66</td>
</tr>
<tr>
<td>Disclosures to Family and Others Involved in Patient’s Care</td>
<td>80</td>
</tr>
<tr>
<td>Business Associates</td>
<td>82</td>
</tr>
<tr>
<td>Marketing</td>
<td>84</td>
</tr>
<tr>
<td>Research</td>
<td>86</td>
</tr>
<tr>
<td>Limited Data Sets</td>
<td>88</td>
</tr>
<tr>
<td>De-Identified Information</td>
<td>90</td>
</tr>
<tr>
<td>Facility Directory</td>
<td>93</td>
</tr>
<tr>
<td>Breach of Unsecured PHI</td>
<td>95</td>
</tr>
<tr>
<td>Privacy Audit Program</td>
<td>99</td>
</tr>
</tbody>
</table>

## SECURITY POLICIES

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Statement of Purpose</td>
<td>101</td>
</tr>
<tr>
<td>HIPAA Compliance Officer Designation</td>
<td>102</td>
</tr>
<tr>
<td>Security Definitions</td>
<td>104</td>
</tr>
<tr>
<td>Topic</td>
<td>Page</td>
</tr>
<tr>
<td>----------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>Device and Media Controls</td>
<td>107</td>
</tr>
<tr>
<td>Facility Access Control Policy</td>
<td>109</td>
</tr>
<tr>
<td>Security Risk Analysis and Risk Management</td>
<td>111</td>
</tr>
<tr>
<td>Integrity and Authentication of ePHI</td>
<td>113</td>
</tr>
<tr>
<td>Contingency Plan for ePHI</td>
<td>115</td>
</tr>
<tr>
<td>HIPAA Security Training &amp; Awareness</td>
<td>117</td>
</tr>
<tr>
<td>Breach of Unsecured ePHI</td>
<td>119</td>
</tr>
<tr>
<td>Business Associates and ePHI</td>
<td>121</td>
</tr>
<tr>
<td>Information Access Management</td>
<td>122</td>
</tr>
<tr>
<td>Technical Safeguards for Access and Audit Controls</td>
<td>124</td>
</tr>
<tr>
<td>Workstation Policy</td>
<td>126</td>
</tr>
<tr>
<td>Working Off-Site</td>
<td>129</td>
</tr>
<tr>
<td>Sanctions</td>
<td>135</td>
</tr>
</tbody>
</table>
Privacy Policies
### I. POLICY\(^1\)

It is the policy of Precision Pain Management of Oklahoma (PPMOK) to protect and safeguard the Protected Health Information (PHI) created, acquired, and maintained by it in accordance with the Privacy Regulations promulgated pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and applicable state laws and as amended by the Health Information Technology for Economic and Clinical Health Act (HITECH).

The Policies are intended to provide guidance to PPMOK Personnel with regard to the protection and enhancement of the privacy rights of patients by:

1. establishing rules related to the internal and external Use and Disclosure of Protected Health Information;
2. affording patients access and information regarding the Use and Disclosure of their Protected Health Information; and
3. implementing administrative procedures intended to assist patients and Personnel to effectuate these Policies.

These Policies supersede and replace any existing conflicting policies and procedures of PPMOK relating to the Use and Disclosure of Protected Health Information. PPMOK may maintain additional policies and procedures relating to the Use and Disclosure of Protected Health Information only to the extent that they do not conflict with these Policies.

The HIPAA Compliance Officer shall promptly notify PPMOK management and staff of any changes in these policies and procedures relating to the Use and Disclosure of Protected Health Information.

**These Policies apply to all PHI, regardless of the form in which it is created or maintained (oral, written, or electronic).**

**These Policies apply to the PHI of both living and deceased patients**

---

\(^1\) These Policies apply to all PHI collected by PPMOK after April 16, 2014.
I. DEFINITIONS Unless otherwise provided, the definitions below apply to all of PPMOK’s Privacy and Security Policies. These terms are capitalized when used in the Policies to indicate that they have been uniquely defined by PPMOK or federal law.

1. **Precision Pain Management of Oklahoma** (PPMOK): Includes its officers, employees, and agents when the context clearly intends such.

2. **Personnel**: Physicians, staff, trainees, and other persons whose conduct, in the performance of work for PPMOK is under the direct control of PPMOK, whether or not they are paid by PPMOK (collectively, the “workforce”). 45 C.F.R. § 160.103.

3. **Authorization**: The formal grant of authority by a patient to a PPMOK to Use or Disclose the patient’s Protected Health Information.

4. **Business Associate**: A person or entity not employed by PPMOK that performs certain functions or activities, or provides certain services for or on behalf of PPMOK that involve the Use and/or Disclosure of a patient’s PHI. Such activities may include, but are not limited to, billing; re-pricing; claims processing and administration; data analysis; legal, accounting, and actuarial services; consulting; utilization review; quality assurance; and similar services or functions. A Business Associate may be a Covered Entity. 45 C.F.R. § 160.103. PPMOK is not prohibited from providing or performing business associate services to a Covered Entity or another Business Associate.

5. **Compliance Date**: The date by which a Covered Entity must comply with the Privacy Regulations, which is April 14, 2003.

6. **Covered Entity**: An entity to which the Privacy Regulations apply, including PPMOK because it is a Health Care Provider that transmits Health Information in electronic form in connection with one of the following eleven transactions:
   a) Health Care claims or equivalent encounter information;
   b) Health Care payment and remittance advice;
c) coordination of benefits;
d) Health Care claims status;
e) enrollment and disenrollment in a health plan;
f) eligibility for a health plan;
g) health plan premium payments;
h) referral certification and authorization;
i) first report of injury;
j) health claims attachments; and
k) other transactions that the Secretary of DHHS may prescribe by regulation. 45 C.F.R. § 160.103.

7. **Covered Functions.** Those functions of a Covered Entity, the performance of which makes the entity a Health Care Provider. 45 C.F.R. § 160.103.

8. **Designated Record Set.** A group of records maintained by or for PPMOK that includes the medical and billing records about individuals or that is used, in whole or in part, by Personnel to make decisions about individuals, regardless of who originally created the information. The definition of a Designated Record Set refers only to the official record for the patient and not to duplicate information maintained in other systems. A Designated Record Set does not include:
a) duplicate information maintained in other systems;
b) data collected and maintained for Research;
c) data collected and maintained for peer review or risk management purposes;
d) Psychotherapy Notes;
e) information compiled in reasonable anticipation of litigation or administrative action;
f) employment records;
g) education records covered by FERPA;
h) information subject to 42 USC 263a (CLIA) or exempt under 42 CFR 493.3(a)(2) (CLIA); and
i) source data interpreted or summarized in the individual's medical record (example: pathology slide and diagnostic films).

9. **Disclose or Disclosure.** The release, transfer, provision of access to, or divulging in any other manner of information outside PPMOK. 45 C.F.R. § 160.103.

10. **Direct Treatment Relationship.** A treatment relationship between an individual and a Health Care Provider that is not an Indirect Treatment Relationship. 45 C.F.R. § 164.501.

11. **Health Care.** Care, services, or supplies related to the health of an individual. Health Care includes, but is not limited to, the following:
a) preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition or functional status of an individual or that affects the structure or function of the body; and
b) sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription. 45 C.F.R. § 160.103.

12. **Health Care Operations.** “Health Care Operations” means any of the following activities of PPMOK to the extent that the activities are related to Covered Functions:
a) Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing Health Care costs; protocol development; case management and care coordination contacting of Personnel and patients with information about treatment alternatives; and related functions that do not include treatment;
b) Reviewing the competence or qualifications of Health Care professionals; evaluating practitioner and provider performance and health plan performance; conducting training programs in which students, trainees, or practitioners in areas of Health Care learn under supervision to practice or improve their skills as Personnel; training of non-Health Care professionals; accreditation, certification, licensing, or credentialing activities;
c) Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;
d) Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating PPMOK, including formulary development and administration, development, or improvement of methods of payment or coverage policies; and
e) Business management and general administrative activities of PPMOK, including, but not limited to:
   i) management activities relating to implementation of and compliance with PPMOK’s Privacy Policies;
   ii) resolution of internal grievances;
   iii) due diligence related to the sale, transfer, merger, or consolidation of all or part of a Health Care Component with another Covered Entity; and
   iv) creating de-identified Health Information or a limited data set. 45 C.F.R. § 164.501.

13. **Health Care Provider:** A provider of services (as defined in § 1861(u) of the Social Security Act, 42 U.S.C. § 1395x(u)), a provider of medical or health services (as defined in § 1861(s) of the Act, 42 U.S.C. § 1395x(s)), and any other person or organization who furnishes, bills, or is paid for Health Care in the normal course of business. 45 C.F.R. § 160.103.
14. **Health Information.** Any information, whether oral or recorded in any form or medium, that:
   
a) is created or received by a Health Care Provider, employer, school or university and
b) relates to the past, present, or future physical or mental health or condition of an individual; the provision of Health Care to an individual; or the past, present, or future payment for the provision of Health Care to an individual. 45 C.F.R. § 160.103.

15. **Health Oversight Agency:** An agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is authorized by law to oversee the Health Care system (whether public or private) or government programs in which Health Information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which Health Information is relevant. 45 C.F.R. § 164.501.

16. **HIPAA** Health Insurance Portability and Accountability Act of 1996. A law which provides a comprehensive and uniform federal standard for the protection of individual health information. It applies to health care plans, health care clearinghouses and certain health care providers (“covered entities”). The law is implemented by the Department of Health and Human Services (HHS) through the adoption of standards, including standards for protecting the privacy and security of individually identifiable health information.

17. **HITECH.** The Health Information Technology for Economic and Clinical Health Act, passed on February 17, 2009.

18. **Hybrid Entity:** A single legal entity: (1) that is a Covered Entity; (2) whose business activities include both Covered and non-Covered functions; and (3) that designates Health Care Components. 45 C.F.R. § 164.504.

19. **Indirect Treatment Relationship:** A relationship between an individual and a Health Care Provider in which: (a) the Health Care Provider delivers Health Care to the individual based on the orders of another Health Care Provider; and (b) the Health Care Provider typically provides services or products or reports the diagnosis or results associated with the Health Care directly to another Health Care Provider, who provides the services or products or reports to the individual. 45 C.F.R. § 164.501.

20. **Individually Identifiable Health Information:** Information that is a subset of Health Information, including demographic information collected from an individual, and that:
a) is created or received by a Health Care Provider, health plan, employer, or health care clearinghouse; and
b) relates to the past, present, or future physical or mental health or condition of an individual;
c) the provision of Health Care to an individual;
d) or the past, present, or future payment for the provision of Health Care to an individual; and
   i) that identifies the individual; or
   ii) with respect to which there is a reasonable basis to believe the information can be used to identify the individual. 45 C.F.R. § 160.103

21. **Law Enforcement Official**: An officer or employee of any agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, or an Indian tribe who is empowered by law to:
   a) investigate or conduct an official inquiry into a potential violation of law; or
   b) prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law. 45 C.F.R. § 164.501.

22. **Marketing**: To make a communication about a product or service that encourages recipients of the communication to purchase or use the product or services unless the communication is made:
   a) to describe a health-related product or service (or payment for such product or service) that is provided by PPMOK, including communications about the entities participating in a Health Care Provider network or health plan network and health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits;
   b) for Treatment of the individual; or
   c) for case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, Health Care Providers, or settings of care to the individual.

23. **Mobile Device**: A mobile device is a computing device that:
   a) Is small enough to be carried by an individual
   b) Is designed to operate without a physical connection (e.g. wirelessly transmit or receive information)
   c) Possesses local removable or non-removable data storage
   d) Includes a self-contained power source
24. **Organized Health Care Arrangement**: A clinically integrated care setting in which the individuals typically receive Health Care from more than one Health Care Provider (example: a hospital and members of its medical staff). 45 C.F.R. § 164.501.

25. **Particularly Sensitive Health Information**: PHI that is generally considered highly confidential including, but not limited to, mental health, drug and alcohol abuse, and communicable disease information.

26. **Payment**: Any activities by PPMOK or a business associate of PPMOK to obtain payment for providing Health Care. Such activities relate to the individual to whom Health Care is provided and include, but are not limited to:
   a) billing, claims management, collection activities, and related Health Care data processing; and
   b) Disclosure to consumer reporting agencies of any of the following PHI relating to collection of premiums or reimbursement:
      i) name and address;
      ii) date of birth;
      iii) social security number;
      iv) payment history;
      v) account number; and
      vi) name and address of the Health Care Provider. 45 C.F.R. §164.501.

27. **Personnel**: Employees, trainees, contract workers, and any other persons whose conduct, in the performance of work for PPMOK, is under the direct control of PPMOK.

28. **Protected Health Information (PHI)**: Individually Identifiable Health Information that is transmitted by, or maintained in, electronic media or any other form or medium. PHI excludes Individually Identifiable Health Information in:
   a) education records covered by the Family Educational Rights and Privacy Act (FERPA); and
   b) employment records held by PPMOK in its role as employer.

29. **Privacy Policies**: This set of policies drafted and adopted by PPMOK for internal use relating to the protection and confidentiality of PHI.

30. **Privacy Regulations**: The regulations issued by the Department of Health and Human Services implementing the privacy requirements of the Health Insurance Portability Act of 1996 (HIPAA), 45 CFR Parts 160 and 164, to protect a patient’s right to privacy in matters involving his or her Health Care, as amended by HITECH.
31. **Psychotherapy Notes**: 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 exclude medication prescription and monitoring, counseling sessions start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date. 45 C.F.R § 164.501.

32. **Public Health Authority**: An agency or authority of the United States, a State, a territory, a political subdivision of a State or territory, an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as part of its official mandate. 45 C.F.R. § 164.501.

33. **Required by Law**: A mandate contained in law that compels PPMOK to make a Use or Disclosure of PHI and that is enforceable in a court of law. Required by Law includes, but is not limited to, court orders and court-ordered warrants; subpoenas or summons issued by a court, grand jury, governmental or tribal inspector general, or administrative body authorized to require the production of information; a civil or an authorized investigative demand; Medicare conditions of participation with respect to Health Care Providers participating in the program; and statutes or regulations that require the production of information, including those that require such information if payment is sought under a government program providing public benefits. 45 C.F.R. § 164.501.

34. **Research**: A systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge. 45 C.F.R § 164.501.

35. **Treatment**: The provision, coordination, or management of Health Care and related services by Personnel. 45 C.F.R. § 164.501. Treatment includes: (a) the coordination or management of Health Care by a Health Care Provider with a third party; (b) consultation between Health Care Providers relating to a patient; or (c) the referral of a patient for Health Care from one Health Care Provider to another. 45 C.F.R. § 164.501.

36. **Use**: With respect to Individually Identifiable Health Information, the sharing, employment, application, utilization, examination, or analysis of such information within PPMOK. 45 C.F.R. § 164.501.
I. PURPOSE: To establish who can act on behalf of the patient for purposes of Authorizing Uses and Disclosures and exercising the patient rights provided by these Policies.

II. POLICY: PPMOK must, except in the limited circumstances set forth in this Policy, treat a Personal Representative as the patient for purposes of Authorizing Uses and Disclosures and exercising the patient rights provided by these Policies. However, the Personal Representative’s decision making authority (and access to PHI) is limited. A Personal Representative’s power is determined by the document which gives him or her authority to act for another person.

PPMOK Personnel are not required to treat the Personal Representative as the patient, if Personnel have a reasonable belief that:

- the Personal Representative has abused or neglected the patient,
- that treating the Personal Representative as the patient could endanger the patient,
- and believe it is not in the patient’s best interest to treat the person as the Personal Representative.

Any questions or concerns should be immediately submitted to the HIPAA Compliance Officer.

Adults: Adults can act as a Personal Representative of another adult if they possess documentation of the following:

1. **Durable Power of Attorney for Health Care:** A durable power of attorney is a document by which the patient may designate an individual as his/her agent to perform certain acts on his/her behalf. Under a valid durable power of attorney, (and depending on the scope of the power of attorney), the agent may make health and medical care decisions on the patient’s behalf. This does not give the agent the power to execute an advance directive for health care, living will, or other document to authorize life-sustaining treatment decisions or to make life-sustaining treatment decisions unless the power of attorney complies with the requirements for a Health Care Proxy. A valid Durable Power of Attorney must be in writing and contain the words “This power of attorney shall not be affected by subsequent disability or incapacity of the principal, or lapse of time,” or “This
power of attorney shall become effective upon disability or incapacity of the principal,” or similar words showing the intent of the principal that the authority conferred will be exercisable notwithstanding the principal’s (patient’s) subsequent disability or incapacity. The document should state whether Personnel may rely on the power of attorney while the patient is still competent or whether it is only effective once the patient becomes incompetent. The patient may revoke the power of attorney at any time if competent. Death of the patient also will revoke and terminate the power of attorney. The execution of a Durable Power of Attorney should be witnessed by two witnesses who are at least 18 years old. The signatures of the patient and witnesses should be notarized.

2. **Power of Attorney**: This differs from a Durable Power of Attorney in that it is only valid so long as the person who granted it is alive, it has not been revoked, and the grantor has his or her mental capacity.

3. **Health Care Proxy**: A Health Care Proxy is an adult appointed by a patient to make health care decisions, including but not limited to withholding or withdrawing of life-sustaining treatment, in certain circumstances pursuant to an advanced directive for health care decision. A Health Care Proxy’s authority becomes effective only
   a. when the patient is incompetent and
   b. has been diagnosed with a terminal condition or as persistently unconscious. The directive must be in writing, signed by the patient, and witnessed by two disinterested witnesses. A disinterested witness is a witness who is at least 18 years old and who does not have an interest in the patient’s estate.
   c. The appointment of the Health Care Proxy may be completely or partially revoked at any time and in any manner by the patient. A revocation is effective upon communication of the desire to revoke to the attending physician or other Personnel. If the patient revokes the advanced directive, a Health Care Proxy may no longer qualify as a Personal Representative.

4. **Court-Appointed Guardian**: This is a person appointed by the court in a court order who legally has authority over the care and management of the person, estate, or both, of a patient who cannot act for him/herself. This order may place certain limitations on the legal activities of the guardian (but it does not have to).

**Minors**: Medical Treatment: For minor patients (under the age of 18) who do not fall within one of the exceptions listed below, either parent, the legal guardian, or the legal custodian appointed by a court may act as a minor’s Personal Representative.

A **minor may act on his/her own behalf in the following instances**:

- Any minor who is married, has a dependent child, or is emancipated.
- Any minor who is separated from his/her parents or legal guardian and is not supported by them.
- Any minor who is or has been pregnant or afflicted with any reportable communicable disease, drug and substance abuse, or abusive use of alcohol, but only if the minor is seeking treatment, diagnosis, or prevention services related to such conditions. If the minor is found not to be pregnant or suffering from a communicable disease, drug or substance abuse, or abusive use of alcohol, Personnel shall not reveal any information to the spouse, parent, or Personal Representative of the minor without the minor’s consent.
- Any minor as to his/her minor child.
- The spouse of a minor if the minor is incapable of consenting because of physical or mental incapacity.
- Any minor who by reason of physical or mental capacity cannot give consent and has no known relatives or legal guardian, if two physicians agree on the health service to be given.
- Any minor in need of emergency services for conditions that will endanger his health or life if delay would result by obtaining consent from his spouse, parent, or legal guardian; provided, however, that the prescribing of any medicine or device for the prevention of pregnancy shall not be considered such an emergency service.

**Note:** A health care provider who provides services to a minor based upon a good faith belief that the minor had the legal ability to consent to the services, and that the consent of the minor’s parents and/or legal guardian is not necessary, is not liable (except for acts of negligence or intentional harm.) A minor who misrepresents his ability to give consent, cannot revoke his consent after receiving services based on his minority.

Except as set forth above, Personnel are required to make a reasonable attempt to inform the spouse, parent, or guardian of the minor of any emergency services provided to the categories of minors set forth above. In all other instances, Personnel may, but are not required to, inform the spouse, parent, or legal guardian of the minor of any treatment provided.

Experimental Procedures/Treatment: Information regarding who may consent for minors to participate in Research and under what circumstances may be obtained from the HIPAA Compliance Officer.

**Deceased Individuals** If under applicable law, there is an executor, administrator, or other person having authority to act on behalf of a deceased individual or of the individual’s estate, that individual must be treated as the Personal Representative of the deceased, with respect to PHI. The court document appointing the individual as an executor or administrator is known as the Letters Testamentary or Letters of Administration and should be signed by a judge. Under Oklahoma law, the following individuals have authority to act as a Personal Representative if there is no executor or administrator appointed: the spouse of the deceased or, if no spouse, any
responsible family member of the deceased. A responsible family member is a parent, adult child, adult sibling, or other adult relative of the deceased who was actively involved in providing or monitoring the care of the deceased, as verified by the doctor, hospital, or other medical institute that was responsible for providing care and treatment of the deceased.

PPMOK must comply with HIPAA with respect to the PHI of deceased individuals for a period of 50 years following the death of the individual.

III. PROCEDURES

1. Personnel must review a copy of the document conferring Personal Representative status to ensure the Personal Representative’s authority is not limited in scope or time and to ensure it meets the requirements described above.
2. Any questions regarding the validity of a document purporting to confer Personal Representative status must be directed to the HIPAA Compliance Officer.
3. Personnel must verify the identity of the individual requesting PHI if the individual is not known. (See Privacy-03, Verification of Identity Policy.)
4. A copy of the written document appointing a person as the Personal Representative of a patient should be placed in the patient’s medical record as verification of the individual’s authority.

IV. REFERENCES

7. Uses and Disclosures of PHI: 45 C.F.R. § 164.502
I. PURPOSE: To help ensure the protection of PPMOK information resources and data by implementing the application of group security policies and configuration management.

II. POLICY: All PPMOK owned or operated computers shall be operated within a suitable Active Directory (AD) and connected to an internal network. As a member of PPMOK’s AD, all computers must be configured as follows:

- Each computer must be named according to an appropriate naming scheme to aid in identification.
- Each computer’s serial number must be listed.
- Each computer’s administrator shall be identified.

DOCUMENTATION: All data collected and/or used as part of the Risk Management Process and related procedures must be formally documented and securely maintained by the HIPAA Compliance Officer.

III. REFERENCES:
1. HIPAA 45 CFR Parts 160, 162, and 164.308(a)(1)(ii)(B)
I. PURPOSE To establish an identity verification process.²

II. POLICY Prior to making a Disclosure or processing a patient request permitted by these Policies, unless otherwise stated in the Policy, Personnel must:

1. verify the identity of a person requesting PHI
2. verify the authority of any such person to have access to PHI, if the identity or any such authority of such person is not known to Personnel; and
3. obtain any documentation, statements, or representations, whether oral or written, from the person requesting the PHI when such documentation, statement, or representation is a condition of the Disclosure or processing.

Subject to III below, to verify identity, Personnel may rely on:

1. An administrative request, including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized under law provided that the information sought is relevant and material to a legitimate Law Enforcement inquiry, the request is specific and limited in scope, and de-identified information could not reasonably be used.

A request by an authorized public official upon presentation of his/her badge or other official credentials if in person or the appropriate letterhead if the request is made in writing. Authority may be verified by written statement or legal process, warrant, subpoena, order, or other legal process.

² Identity verification process is not required for Disclosure to family members or others involved in the patient’s care, and when the patient has given PPMOK written authorization to Disclose Information to a given person.
2. Personal judgment if a Disclosure is being made only to avert a serious threat to health or safety or in cases when a patient is required to be given an opportunity to agree or object to the Disclosure.

**Verification of identity can be accomplished by:**

- review of picture I.D.;
- review of credentials or badge;
- signature comparison; or
- If the individual’s identity cannot be verified through any of these methods, please contact the HIPAA Compliance Officer for guidance.

*After verifying the individual’s identity, we must still determine whether the individual is authorized to obtain PHI.*

**III. PROCEDURES** Any questions regarding verification of or reliance on identity or authority should be directed to the HIPAA Compliance Officer. The HIPAA Compliance Officer should be contacted prior to responding to any request by law enforcement officials.

**IV. REFERENCES:**

1. See also Uses and Disclosures – Required by Law) for additional information on releases to law enforcement and in response to subpoenas.

2. 45 C.F.R. §164.514 (h) (1).
Notice of Privacy Practices

<table>
<thead>
<tr>
<th>Subject: Notice of Privacy Practices</th>
<th>Page: 1 of 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy #: Privacy-05 (Patient Rights)</td>
<td>Approved: May 23, 2014</td>
</tr>
<tr>
<td>Effective Date: May 30, 2014</td>
<td>Revised:</td>
</tr>
<tr>
<td>Next Review Date: July 31, 2014</td>
<td>Reviewer:</td>
</tr>
</tbody>
</table>

I. PURPOSE  To require the development and distribution of a Notice of Privacy Practices (NPP).

II. POLICY  The HIPAA Compliance Officer shall develop and distribute a NPP for PPMOK which includes the information required by the Privacy Regulations. A patient’s receipt of the NPP must be acknowledged.

The NPP must be translated into other languages as required by regulations issued by the Office for Civil Rights regarding accommodations for people with Limited English Proficiency.

Personnel may not use or disclose PHI in a manner inconsistent with the PPMOK’s NPP.

III. PROCEDURE

**Acknowledgement:** Personnel must make a good faith effort to obtain a written acknowledgement of the receipt of the Notice of Privacy Practices:

- Each patient must be given a NPP upon arrival for their first appointment, and once per year thereafter.
- Ask the patient to sign the Acknowledgment of Receipt of NPP.
- If the patient does not acknowledge receipt of the NPP, make a note on the registration form or in the patient’s medical record indicating why the acknowledgement was not obtained.
- PPMOK will not condition Treatment on the patient’s acknowledgement of the receipt of the NPP.

**Distribution:** PPMOK shall make the NPP available to any person who requests it. PPMOK Personnel must:

---

3 (See Acknowledgement of Receipt of Notice of Privacy Practices form.)
1. Provide the NPP to each patient on or before the date of first service, including service delivered electronically. If the first service delivery to an individual is delivered electronically, a provider must provide an electronic copy of the NPP in its first response to the individual’s first request for service. During emergency treatment situations, the NPP may be provided and the acknowledgement obtained as soon as reasonably practicable after the emergency treatment situation is resolved.

2. Make the NPP available at the service delivery site upon request.

3. The NPP must be posted, or made available in the lobby/waiting area of each health care provider.

4. The NPP may be distributed by e-mail if the patient agrees to the electronic notice⁴. The Notice should be sent to the patient contemporaneously with PPMOK’s first electronic communication to the patient. If Personnel have reason to believe the electronic transmission has failed, a hard copy must be provided. When electronic notice is provided, an Acknowledgement of Receipt of NPP must be obtained.

5. Health Care Providers with Indirect Treatment Relationships with patients shall provide the NPP to individuals upon request.

6. The NPP for PPMOK must be posted and made available electronically on the web site of PPMOK.

**Amendment of the Notice of Privacy Practices** If the NPP is amended, upon going into effect, the amended version of the NPP must be made available upon request to current patients. Unless specifically instructed by the HIPAA Compliance Officer, Personnel do not have to obtain a new acknowledgement from current patients.

**Retention** The NPP shall be retained by the HIPAA Compliance Officer for six years.

**IV. REFERENCES**

1. AMC HIPAA Privacy Guidelines, PRIV. 43 (pg. 167-172).
2. HIPAA Privacy Regulations, 45 C.F.R. 520

---

⁴ (See Electronic NPP form.)
I. PURPOSE To manage patient access to Protected Health Information.

II. POLICY

Rights to Access: PPMOK will permit patients to inspect and obtain a copy of their PHI that is included in a Designated Record Set and maintained by PPMOK, for as long as the PHI is maintained in the Designated Record Set. If the same information is kept in more than one Designated Record Set or in more than one location, PPMOK must produce the information only once per request for access.

Unless an exception applies, a patient should be granted access to the entire medical record, including records received from other providers that were used to make Treatment decisions.

PPMOK may charge a fee for access to PHI as long as the fee includes only the costs of copying and postage and is consistent with any limit set by State law.

State law currently permits a charge of $.50 for each page for paper records and $5.00 per film for radiology films, plus postage. Records produced in digital form are $.30 per page, so long as the entire record is produced and delivered electronically.

PPMOK must provide the patient with access to PHI in the form or format requested by the patient, if it is readily producible in such form or format; or, if not, in a readable hard copy form or such other form or format as agreed to by PPMOK and the patient. If the PHI is maintained in an electronic health record, PPMOK must provide the patient with a copy of the PHI in electronic format, upon request.

PPMOK must arrange with the patient for a convenient time and place to inspect or obtain a copy of the PHI or mail a copy of the information at the patient’s request. PPMOK may discuss
the scope, format, and other aspects of the request for access with the patient as necessary to facilitate the timely\(^5\) provision of access.

If PPMOK does not maintain the PHI that is the subject of the patient’s request for access and Personnel know where the requested information is maintained, then PPMOK must inform the patient where to direct the request for access.

**Psychotherapy Notes\(^6\):** At this time PPMOK does not maintain psychotherapy notes, but in the event that it should maintain them at some time: A patient does not have the right to access Psychotherapy Notes relating to him/herself except (i) to the extent the patient’s treating professional approves such access in writing; or (ii) the patient obtains a court order authorizing such access.

**Denial of Right to Access:** A patient may be denied access to PHI under the limited circumstances listed below. The following exceptions should be narrowly construed and rarely used:

**Legal Information:** PPMOK may deny a patient access to information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding. The advice of legal counsel should be obtained prior to denying a patient’s request for access on this basis.

**Research:** PPMOK may temporarily suspend a patient’s access to PHI created or obtained in the course of Research that includes Treatment. The suspension may last for as long as the Research is in progress, provided that the patient has agreed to the denial of access when consenting to participate in the Research and the patient has been informed that the right of access will be reinstated upon completion of the Research.

**Information from Other Source:** PPMOK may deny a patient’s access to PHI if the information was obtained from someone other than a Health Care Provider under a promise of confidentiality and the access requested would be reasonably likely to reveal the source of the information.

**Endangerment:** PPMOK may deny a patient access to PHI in the event a licensed Health Care Professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the patient or another person. Access may not be denied on the basis of the sensitivity of the Health Information or the potential for causing emotional or psychological harm.

**Reference to Other People:** PPMOK may deny a patient access to PHI if it makes reference to another person and a licensed Health Care Professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to cause substantial harm to

---

\(^5\) For purposes of this Policy, a timely provision of access shall be considered to be any time within thirty (30) calendar days of a valid request for access.

\(^6\) See Psychotherapy Notes, Definitions; and Mental Health.)
such other person. Access can be denied if the release of such information is reasonably likely to cause substantial physical, emotional, or psychological harm to the other person.

**Personal Representative**: PPMOK may deny access to PHI if the request is made by a patient’s Personal Representative and a licensed Health Care Professional has determined, in the exercise of professional judgment, that the provision of access to such Personal Representative is reasonably likely to cause substantial harm to the patient or another person, or likely to perpetuate fraud or financial abuse of an incapacitated or vulnerable person.

**CLIA Information**: PPMOK may deny access to PHI that is subject to 42 USC 263a if such access would be prohibited by law, or to PHI that is exempt under 42 CFR 493.3(a)(2), CLIA.

**Privacy Act**: PPMOK may deny access to PHI that is in records subject to the Privacy Act, if denial meets the requirements of the Act. Contact PPMOK’s HIPAA Compliance Officer prior to denying access on this basis.

**PPMOK must, to the extent possible, give the patient access to any other PHI requested, after excluding the PHI to which access is being denied.**

**Review of Denied Access**: If access to PHI is denied, the patient must be given the opportunity to have the denial reviewed by either the supervisor of PPMOK or the HIPAA Compliance Officer. The Denial of Individual’s Request for PHI form must be used to ensure this information is provided to the individual. The person reviewing the denial cannot have participated in the original denial.

**III. PROCEDURES**

**Rights to Access**: All patients must make their requests for access in writing using either PPMOK’s Authorization for Release of Medical Information form (Authorization form) or another form that complies with HIPAA and state law. Patients making their request for access by telephone or e-mail should be sent a copy of the form. The form must be maintained in the patient’s medical record for a minimum of six (6) years.

1. Upon receipt of a request for access, PPMOK should provide the patient with the Authorization form. PPMOK should then process the request. If the request is denied, a copy of the Denial form, if applicable, should also be filed in the patient’s medical record and, sent to the HIPAA Compliance Officer.
2. A patient’s request for access to PHI must be acted upon as soon as reasonably possible, but in no event more than thirty (30) calendar days after receiving the request.
3. The supervisor of PPMOK shall be responsible for receiving and processing requests for access to PHI.
4. Any questions regarding a patient’s right of access should be forwarded to the HIPAA Compliance Officer.

---

**The Health Care Provider who treated the patient should be notified by PPMOK if a patient requests access to his/her PHI for litigation or some other unusual purpose.**
**Denial of Right to Access:** If a patient’s request for access to PHI is denied, the supervisor shall prepare a written denial using PPMOK’s Denial of Request for Protected Health Information form. The patient must be provided a copy of the denial within thirty (30) days of his or her request for access. The form must be maintained in the patient’s medical record for a minimum of six (6) years. The copy forwarded to the HIPAA Compliance Officer also should be maintained for six (6) years.

**Review of Denied Access:** PPMOK is required to promptly forward requests for review of denial to the HIPAA Compliance Officer, and the HIPAA Compliance Officer is required to review the denial within a reasonable period of time, but no later than thirty (30) days after receiving the request for review. Access to PHI must be provided to the patient in accordance with the determination of the Compliance Officer. The patient making the request should be notified promptly, in writing, of the Compliance Officer’s decision, a copy of which must be filed in the patient’s medical record and maintained for six (6) years, and an additional copy shall be maintained by the Compliance Officer for six (6) years.

**IV. REFERENCES**

1. AMC HIPAA Privacy Guidelines, PRIV. 45 (pg. 175).
2. HIPAA Privacy Regulations, 65 45 C.F. R. 164.524(a)
I. PURPOSE  To permit patients to request an accounting of the Disclosures of their PHI.

II. POLICY  PPMOK will permit patients to request an accounting of Disclosures of their PHI maintained by it. The accounting must include Disclosures made by PPMOK in the six (6) years prior to the date of the request (unless limited at the request of the patient), including Disclosures to or by Business Associates.

Accounting Requirements – General  The accounting must include all Disclosures, except for Disclosures:

- to carry out Treatment, Payment, or Health Care Operations;
- to patients of Protected Health Information about them;
- incident to a Use or Disclosure otherwise permitted or required by the Privacy Regulations;
- pursuant to the patient’s Authorization and Patient Access to PHI;
- to persons involved in the patient’s care, or to notify or assist in the notification of a family member, Personal Representative, or other responsible for the care of the patient of the patient’s location, general condition, or death;
- for national security or intelligence purposes;
- to Correctional Institutions or Law Enforcement officials to provide them with information about a person in their custody;
- as part of a limited data set (see Privacy 31-Limited Data Sets); or
- that occurred prior to April 15, 2003.

Examples of Disclosures subject to the accounting requirement include but are not limited to Disclosures for, or pursuant to:

1. Research, unless, Authorized by patient;
2. subpoenas, court orders, or discovery requests;
3. abuse and/or neglect reporting;
4. communicable disease reporting; or
5. other reports to the Department of Health such as tumor registry.

Suspension of Accounting  A patient’s right to receive an accounting of Disclosures must be suspended at the request of a Health Oversight Agency or Law Enforcement Official if certain conditions are satisfied. If PPMOK receives a request to suspend a patient’s right to receive an accounting from a Health Oversight Agency or Law Enforcement Official, PPMOK’s HIPAA Compliance Officer should be contacted to determine if the appropriate conditions have been satisfied.

III. PROCEDURE  A patient must request an accounting of Disclosures in writing using the Request for Accounting of Disclosure form. Patients making their request for an accounting by telephone or e-mail should be forwarded a copy of the form. The request form must be maintained in the patient’s medical record for a minimum of six (6) years.

Request for Accounting of Disclosures:  Upon receipt of a request for an accounting of Disclosures, PPMOK should:

1. Provide the patient with the appropriate form.
2. Verify the identity of the person making the request.
3. Process the request in accordance with its internal procedures and send a copy of the request form and a copy of the Accounting of Disclosures log to the HIPAA Compliance Officer.
4. Administrative:

1. An Accounting of Disclosure Log must be used to record Disclosures and must be maintained in a patient’s medical record for a period of at least six (6) years from that date of the last accounting. For each Disclosure that must be recorded, the accounting log must include the following information:
   a. the date of the Disclosure;
   b. the name of the entity or person who received the PHI and, if known, the address of such entity or person;
   c. a brief description of the PHI that was Disclosed; and
   d. a brief statement of the purpose of the Disclosure that reasonably informs the patient of the basis for the Disclosure, or a copy of the written request for the Disclosure, if approved by HIPAA Compliance Officer.
2. The Request for Accounting of Disclosures form and the log forwarded to the HIPAA Compliance Officer, and should be maintained for six (6) years in the patient’s record, and by the Compliance Officer.
3. The supervisor of PPMOK shall be responsible for processing requests for accounts of Disclosures.
a. If the supervisor of PPMOK cannot perform any of the duties listed herein for any reason, then he or she shall immediately notify the HIPAA Compliance Officer in writing, and request their assistance. The supervisor of PPMOK is responsible for ensuring requests are processed appropriately and in a timely manner, and that Accounting of Disclosure Logs are maintained.

4. If during the period covered by the accounting PPMOK has made multiple Disclosures of PHI to the same person or entity for a single purpose, or pursuant to a single Authorization, the accounting may, with respect to such multiple Disclosures and upon approval of the HIPAA Compliance Officer, provide:
   a. the information set forth in section 4 above for the first Disclosure during the accounting period;
   b. the frequency, periodicity, or number of the Disclosures made during the accounting period; and
   c. the date of the last such Disclosure during the accounting period.

5. If during the period covered by the accounting PPMOK has used a Business Associate, PPMOK must contact the Business Associate to obtain an Accounting of Disclosures made by the Business Associate. This accounting must also be provided to the patient.

6. PPMOK will act on the patient’s request for an accounting no later than sixty (60) calendar days after receipt of such a request. If PPMOK is unable to meet this deadline, it must contact the HIPAA Compliance Officer to request an extension, which may not exceed 30 calendar days. The Compliance Officer will be responsible to the patient regarding an extension.

7. The first accounting to a patient in any twelve-month period must be provided at no charge. PPMOK may impose a reasonable, cost-based fee for each subsequent request for an accounting by the same patient within the twelve-month period, provided that PPMOK informs the patient in advance of the fee and provides the patient with an opportunity to withdraw or modify the request for a subsequent accounting in order to avoid or reduce the fee.

IV. REFERENCES

1. AMC HIPAA Privacy Guidelines, PRIV. 47 (pg. 185).
2. HIPAA Privacy Regulations, 45 C.F. R. 164.528

7 (See Privacy 05 for fees.)
I. PURPOSE To permit patients to request communication of PHI by alternative means or at alternative locations.

II. POLICY PPMOK will permit patients to request, and will accommodate reasonable requests by patients, to receive communications of PHI by alternative means or at alternative locations.

PPMOK shall not require an explanation from the patient as to the basis for the request as a condition of considering or granting the request.

The HIPAA Compliance Officer shall be responsible for determining if a particular request for alternative means of communication is reasonable in light of the expense and administrative burden involved with complying with the request.

PPMOK may condition the provision of an alternative means of communication on receiving: (a) information as to how payment will be handled, if applicable and (b) the specification of an alternative address or other method of contact.

Requests: Requests for communication by alternative means or at alternative locations may only be submitted using the Request for Communication by Alternative Means form.

If a request for communication by alternative means is granted, PPMOK must:

1. communicate with the patient in accordance with the patient’s request.
2. must place or affix a clear indication of the communication by alternative means on the patient’s medical record, whether it paper or electronic form.

III. PROCEDURE

1. A patient must request communication by alternative means or at alternative locations in writing by using the Request for Communication by Alternative Means form.

---

8 (available on the HIPAA forms web page)
2. Upon receipt of a request for communication by alternative means, PPMOK should provide the patient with the appropriate form.

3. The PPMOK supervisor shall promptly submit the request form to the HIPAA Compliance Officer for processing.
   a) The Compliance Officer shall explain any limitations or reasons for denial of the request in writing, and shall return the written explanations with the processed Request form to PPMOK.

4. The Compliance Officer shall prepare (and send) a letter to the patient explaining a denial or limitation on the request and the reasons therefore.

5. The Compliance Officer shall return the processed Request to PPMOK, and a copy of the form and the letter shall be placed in the patient’s medical records.
   a) if the request is denied, the HIPAA Compliance Officer shall provide the patient with a copy of the Request form with the reason for the denial noted.
   b) If the patient cannot be notified of the denial before his/her next appointment, the Request form, with the explanation of denial, should be sent to the patient as soon as possible.
   c) In order to protect the patient, the denial should be sent to the alternative address, if specified, for this communication only.

6. Requests for alternative means of communication and documentation of any denials, or limitations of such requests shall be maintained in a patient’s medical record for a minimum of six (6) years. The HIPAA Compliance Officer shall only maintain a record of denials and corresponding letters for six (6) years in addition to the copy maintained in the patient’s medical records.

7. To ensure that agreed upon alternative means of communication are communicated to the providers and business associates who may be sending the patient communications on behalf of the PPMOK, the PPMOK supervisor must send those entities a copy of the approved Request form.

IV. REFERENCES

1. AMC HIPAA Privacy Guidelines, PRIV. 44 (pg. 173).
2. HIPAA Privacy Regulations, 45 C.F.R. 164.522

9 (available on the PPMOK web page)
I. PURPOSE To permit patients to request amendments to their Protected Health Information.

II. POLICY PPMOK will permit patients to request amendments to their PHI contained in a Designated Record Set.

PPMOK may deny a patient’s request for amendment if it determines that the PHI (or record) which is the subject of the request:

1. was not created by PPMOK, unless the patient provides a reasonable basis to believe that the originator of PHI is no longer available to act on the requested amendment;
2. is not part of the Designated Record Set;
3. is not available for inspection by the patient pursuant to Patient Access to Protected Health Information Policy;
4. is accurate and complete.

Patients requesting an amendment to their PHI must provide a reason to support a requested amendment. See Request for Amendment of PHI form, available on the HIPAA website.

III. PROCEDURE

1. Patients must request amendments to their PHI in writing by using PPMOK’s Request for Amendment of Protected Health Information form. Patients making their request for an amendment by telephone or e-mail should be sent a copy of the form. Verification of the requester’s identity must be obtained prior to considering the amendment request. The request form must be maintained in the patient’s medical record for a minimum of six (6) years.

2. Upon receipt of a request for an amendment, PPMOK should process the request in accordance with its internal policy and file a copy of the request in the patient’s medical record.
3. The PPMOK supervisor shall be responsible for processing amendment requests. The specific individual responsible for recording the PHI or originating the record must be consulted, if possible, and should sign the amendment form.

4. PPMOK must act on the patient’s request no later than sixty (60) calendar days after receipt of a request, as set forth below:
   a) Accepting the Amendment. If PPMOK accepts the requested amendment, in whole or in part, it must:
      i) make the appropriate amendment by identifying the records in the Designated Record Set that are affected by the amendment and appending or providing a link to the amendment to such record;
      ii) inform the patient, in writing, that the amendment is accepted by sending the patient a copy of the completed Request for Amendment form with the acceptance noted;
      iii) obtain the patient’s agreement to have PPMOK notify the relevant persons with whom the amendment needs to be shared by using the form; and
      iv) make reasonable efforts to inform and provide the amendment within a reasonable time to persons identified by the patient as having received PHI about the patient and needing the amendment, and persons as well as Business Associates that PPMOK knows have the PHI that is the subject of the amendment and who may have relied, or could foreseeably rely, on such information to the detriment of the patient.
   b) Denying the Amendment. If PPMOK denies the requested amendment, in whole or in part, it must:
      i) inform the patient, in writing, that the amendment is denied by sending the patient a copy of the completed Request for Amendment form, and a letter explaining the reasons for the denial;
      ii) permit the patient to submit a written statement disagreeing with the denial of all or part of a requested amendment and the basis of such disagreement;
      iii) identify, as appropriate, the record or PHI in the Designated Record Set that is the subject of the disputed amendment and append or otherwise link the patient’s request for an amendment; PPMOK’s denial of the request; the patient’s statement of disagreement, if any; and PPMOK’s rebuttal, if any, to the Designated Record Set. (PPMOK may, but is not required to, prepare a written rebuttal to the patient’s statement of disagreement. If a rebuttal statement is prepared, a copy of it must be provided to the patient who submitted the statement of disagreement.) The HIPAA Compliance Officer must be contacted prior to sending the rebuttal.

5. If a statement of disagreement has been submitted by the patient, PPMOK must include the material set forth in subsection (iii) of the preceding paragraph or, at its election, an accurate summary of any such information, with any subsequent Disclosure of PHI to which the disagreement related.
6. If the patient has not submitted a written statement of disagreement, PPMOK must include the patient’s request for amendment and its denial, or an accurate summary of such information, with any subsequent Disclosure of PHI only if the patient has requested such action.

7. If PPMOK is informed by another Covered Entity of an amendment to a patient’s PHI must amend the PHI in its Designated Record Sets.

8. Requests for amendments and documentation of the response to such requests must be maintained in a patient’s medical record for a minimum of six (6) years.

IV. REFERENCES

1. AMC HIPAA Privacy Guidelines, PRIV. 46 (pg. 181).
2. HIPAA Privacy Regulations, 45 C.F.R. 164.526 (a).
Right to Request Restriction on Use and Disclosures

<table>
<thead>
<tr>
<th>Subject: Right to Request Restriction on Use and Disclosures</th>
<th>Page: 1 of 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy #: Privacy-10 (Patient Rights)</td>
<td>Approved: May 23, 2014</td>
</tr>
<tr>
<td>Effective Date: May 30, 2014</td>
<td>Revised:</td>
</tr>
<tr>
<td>Next Review Date: July 31, 2014</td>
<td>Reviewer:</td>
</tr>
</tbody>
</table>

I. PURPOSE To permit patients to request restrictions on the Use and Disclosure of their PHI.

II. POLICY

1. PPMOK will permit patients to request restrictions on the Use and Disclosure of their PHI:
   a) to carry out Treatment, Payment, or Health Care Operations and/or
   b) to people involved in their care or for notification purposes as described in § 164.510(b) of the Privacy Regulations.

2. PPMOK is not required to agree to any request to restrict the Use and Disclosure of PHI unless the Disclosure is to a health plan for purposes of Payment or Health Care Operations and the PHI pertains to a health care item or service for which the provider has been paid out-of-pocket in full.

3. If PPMOK agrees to a restriction, it will not Use or Disclose PHI in violation of the restriction, except in emergency situations when the PHI is needed to treat the patient. If restricted PHI is Disclosed to a Health Care Provider for emergency treatment, PPMOK (at the time of) disclosing the information shall request that the Health Care Provider who received the information not further Use or Disclose the information.

4. Any agreed-upon restriction will not prevent Uses and Disclosures to the patient or as Required by Law.

5. PPMOK shall adhere to any agreed-upon restriction until the restriction is terminated according to the procedures set forth below.

6. Personnel may not Use or Disclose PHI that is subject to a restriction, except to provide emergency treatment or as Required by Law.

7. The HIPAA Compliance Officer shall determine whether a particular restriction should be permitted.

III. PROCEDURE

1. Patients must request restrictions on the Use and Disclosure of their PHI in writing by using the Request for Restriction on Use and Disclosures of Protected Health Information form.
2. Verification of the requester’s identity must be obtained prior to considering the request.
3. Upon receipt of a restriction request, PPMOK should provide the patient with the Request for Restriction form. PPMOK should process the request in accordance with its internal procedures and file a copy of the request form in the patient’s medical record.
4. Requests for restrictions that are not Required by Law to be granted should generally be granted only in rare instances in which the facts and circumstances indicate such a restriction is necessary to protect the patient.
5. Completed Request forms and should be submitted to the HIPAA Compliance Officer for processing.
6. The HIPAA Compliance Officer shall notify the patient in writing if the request is denied by providing the patient with a copy of the completed Request for Restriction form that includes the reason for the denial. If the patient cannot be notified of the denial at the time of his/her next visit, the form, with the denial noted, and letter should be sent to the patient.
7. Requests for restrictions and documentation of approvals or denials of such requests should be maintained in a patient’s medical record and by the HIPAA Compliance Officer for a minimum of six (6) years.
8. To ensure that agreed-upon restrictions on the Use and Disclosure of PHI are communicated to the billing department and other departments, providers, and Business Associates who may be Using or Disclosing the patient’s PHI on behalf of PPMOK and/or Health Care Provider who agreed to the request, PPMOK must send those departments and entities a copy of the approved Request form.
9. A restriction on the Use and Disclosure of PHI that is not Required by Law can be terminated if
   a) the patient requests the termination in writing;
   b) the patient orally agrees to or requests the termination and the oral request or agreement is documented in the patient’s medical record and communicated in writing to the HIPAA Compliance Officer; or
   c) PPMOK informs the patient that it is terminating its agreement to the voluntary restriction, in which case the termination will apply only to PHI created or received after the patient has been notified of the termination. The Revocation of Request for Restriction and Use and Disclosure of PHI form, available on the PPMOK website, may be used.
10. If a restriction request is granted, PPMOK must place or affix a clear indication of the restriction on the patient’s medical record, whether it is in paper or electronic form.

IV. REFERENCES

1. AMC HIPAA Privacy Guidelines, PRIV. 11.
2. HIPAA Privacy Regulations, 45 C.F. R. 16
I. PURPOSE To provide for the designation of a HIPAA Compliance Officer, and to set forth contact information as required by the Privacy Regulations.

II. POLICY PPMOK’s HIPAA Compliance Officer is responsible for the development and implementation of its Privacy Policies, and shall be responsible for answering questions regarding the content of its Privacy Policies and Notice of Privacy Practices. The HIPAA Compliance Officer shall also be responsible for receiving and managing the investigation of complaints regarding HIPAA compliance and the Notice of Privacy Practices.

III. PROCEDURE

1. Documentation regarding the designation of the HIPAA Compliance Officer and his/her contact information must be retained, in written or electronic format, for at least six (6) years by PPMOK.

2. The contact information for the HIPAA Compliance Officer is set forth on PPMOK’s web pages and will be revised in the event a new HIPAA Compliance Officer is designated or the contact information changes.

3. The HIPAA Compliance Officer is:
   Valerie L. Dye
   P: (918) 359-5948
   C: (918) 852-0695

IV. REFERENCES

1. AMC HIPAA Privacy Guidelines, PRIV. 48 and 49 (pg. 190-193).
2. HIPAA Privacy Regulations, 45 C.F.R. 164.530
I. PURPOSE: To establish procedures for individuals to submit privacy complaints, and any all.

II. POLICY: All incidents regarding HIPAA Policies, shall be documented, reviewed, and acted upon, if necessary, by the Compliance Officer. Complaints must be reported on the Privacy Complaint form.

Documentation regarding complaints received and the resolution of such complaints will be retained, in written or electronic format, for at least six (6) years by the HIPAA Compliance Officer.

III. PROCEDURE: All Privacy incidents shall be immediately reported to the HIPAA Compliance Officer.

1. PPMOK shall immediately report any privacy complaint to the Compliance Officer, and assist the Compliance Officer in investigating complaints.
2. PPMOK shall track privacy complaints received by keeping a written log of the date, time, and relevant details regarding the complaint. Emailing the Compliance Officer may be considered a sufficient log.
3. The Compliance Officer and PPMOK will document each complaint received and maintain such documentation for at least six (6) years.
4. The Compliance Officer shall be responsible for the investigation of each complaint.
5. PPMOK and the Compliance Officer shall each maintain a record of each Privacy incident, the investigation, and the resolution. PPMOK shall provide a copy of its record to the Compliance Officer annually, and upon request.

IV. REFERENCES

1. AMC HIPAA Privacy Guidelines, PRIV. 52 (pg. 198).
2. HIPAA Privacy Regulations, 45 CFR §164.530.
I. PURPOSE: To establish documentation requirements as required by the Privacy Regulations.

II. POLICY: PPMOK will maintain, for at least six (6) years, the following:

- Written or electronic copies of its Privacy Policies;
- Written or electronic copies of any communication that is required by the Privacy Regulations to be in writing; and
- Written or electronic records of any action, activity, or designation that is required by the Privacy Regulations to be documented.

III. PROCEDURE:

1. Documentation of Privacy Policies. Written or electronic copies of PPMOK’s Privacy Policies will be maintained by the HIPAA Compliance Officer for at least six (6) years from the date any such Policies were created or were last in effect, whichever is later.

2. Documentation of Communications Required by the Privacy Regulations. Documentation will be retained for a period of at least six (6) years from the date of creation in the location specified in the particular Privacy Policy in which such communication is specifically addressed.

3. Documentation of Any Action, Activity, or Designation Required by Privacy Regulations will be retained for a period of at least six (6) years from the date of creation in the location specified in the particular Privacy Policy in which such action, activity, or designation is specifically addressed.

IV. REFERENCES:

1. AMC HIPAA Privacy Guidelines, PRIV. 59 (pg. 211-212).
2. HIPAA Privacy Regulations, 45 C.F.R. 164.530 (j)
I. PURPOSE: To prohibit retaliation and intimidation against individuals who exercise their rights under the Privacy Regulations.

II. POLICY: PPMOK and its Personnel shall not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against an individual who:

1. Exercises any right under, or participates in, any process established by the Privacy Regulations;
2. Files a complaint with the Secretary of the Department of Health and Human Services as permitted by the Privacy Regulations;
3. Testifies, assists, or participates in an investigation, compliance audit or review, proceeding, or hearing conducted by PPMOK or a government enforcement agency under the Privacy Regulations; or
4. Opposes any act or practice made unlawful by the Privacy Regulations, provided the individual has a good faith belief that the practice opposed is unlawful and the manner of the opposition is reasonable and does not involve a Disclosure of PHI in violation of the Privacy Regulations or PPMOK’s Privacy Policies.

III. PROCEDURE: Any individual who believes that some form of retaliation or intimidation against an individual for exercising rights under the Privacy Regulations is occurring or has occurred should report the incident to the HIPAA Compliance Officer.

If the individual feels that the HIPAA Compliance Officer is involved in the retaliation or intimidation, then the individual should report the incident to a member of management not involved in the incident.

---

10 For purposes of this Policy, the term “individual” is not limited to natural persons, but includes any type of organization, association, or group such as other Covered Entities, Health Oversight Agencies, and advocacy groups...
Upon receipt of a report of retaliation or intimidation, the HIPAA Compliance Officer will conduct an investigation to determine if retaliation or intimidation has occurred. If the report is substantiated, Sanctions shall be imposed in accordance with company policies and the Privacy Policies.

IV. REFERENCES:

1. AMC HIPAA Privacy Guidelines, PRIV. 55 (pg. 204-205).
2. HIPAA Privacy Regulations, 45 CFR 164.530(g) and 45 CFR 160.316.
I. PURPOSE: To establish procedures regarding the mitigation of harmful effects of inappropriate Uses or Disclosures of PHI.

II. POLICY: PPMOK will mitigate, to the extent practicable, any known harmful effect of a Use or Disclosure of PHI in violation of PPMOK’s Privacy Policies.

III. PROCEDURE: PPMOK must take practicable steps to mitigate the harmful effects of an inappropriate Use or Disclosure. The type of mitigation that occurs will be based on the facts and circumstances of each case, based on the following factors:

1. knowledge of where the PHI has been disclosed;
2. how the PHI might be used to cause harm to the patient or another individual; and
3. what steps can actually have a mitigating effect under the facts and circumstances.

PPMOK must investigate the cause of the inappropriate Use or Disclosure and take corrective actions to prevent such Uses or Disclosures from re-occurring. The investigation shall be conducted, in part, to identify methods for effective mitigation.

1. PPMOK shall notify the HIPAA Compliance Officer, in accordance with Privacy Complaint Reporting and Tracking, of Inappropriate Uses and Disclosures, the results of the investigation, and the proposed mitigation efforts. Once mitigation is determined, the HIPAA Compliance Officer shall confirm it has been implemented.
2. If legal action is threatened or is a distinct possibility, legal counsel shall be notified.

IV. REFERENCES:

1. AMC HIPAA Privacy Guidelines, PRIV. 54 (pg. 202-203).
2. HIPAA Privacy Regulations, 45 CFR 164.530(f).
I. PURPOSE: To outline the requirements for changes to PPMOK’s Notice of Privacy Practices and amendment of its Privacy Policies.

II. POLICY: PPMOK, through its HIPAA Compliance Officer, will promptly change its Notice of Privacy Practices and amend its Privacy Policies as necessary and appropriate to comply with changes in the law, including the Privacy Regulations, or to accommodate changes in the structure or operations of PPMOK.

PPMOK has reserved, in its Notice of Privacy Practices, the right to change its Privacy practices and amend its Privacy Policies. Therefore, any such changes or amendments will be effective for PHI created or received by PPMOK after the effective date of the amendment.

III. PROCEDURE:

Changes to Privacy Practices and Policies Addressed in the Notice of Privacy Practices. In order to effectuate changes to Privacy practices and Policies addressed in the Notice of Privacy Practices, PPMOK, through its HIPAA Compliance Officer, will:

1. Ensure that the Privacy Policies, if revised to reflect a change in the PPMOK’s Privacy practices, comply with the Privacy Regulations and applicable state laws.
2. Document the revised Privacy Policy, in written or electronic format, and retain such documentation for at least six (6) years.
3. Revise PPMOK’s Notice of Privacy Practices as required by the Privacy Regulations to state the changed practice and make the revised Notice available as required. PPMOK shall not implement an amendment to a Privacy Policy addressed in the Notice of Privacy Practices prior to the effective date of the revised Notice.

Amendments to Privacy Policies Not Addressed in the Notice of Privacy Practices. PPMOK may amend, at any time, a Privacy Policy that does not materially affect the content of its Notice of Privacy Practices. In order to effectuate such an amendment, PPMOK, through its HIPAA Compliance Officer, will:
1. Ensure that the Privacy Policy, as amended, complies with the Privacy Regulations; and
2. Document the revised Privacy Policy, in written or electronic format, and retain such documentation for at least six (6) years.
3. Notify Personnel of significant changes in policies and/or practices and provide training updates as necessary.

IV. REFERENCES:

1. AMC HIPAA Privacy Guidelines, PRIV. 58 (pg. 208-210).
2. HIPAA Privacy Regulations, 45 C.F.R. 164.530(i)
I. PURPOSE: To prohibit any requirement for or effort to require patients to waive their rights under the Privacy Regulations.

II. POLICY: PPMOK will not require patients to waive:

1. their right to file a complaint with the Secretary of the Department of Health and Human Services or
2. any other enforcement agency regarding PPMOK’s compliance with the Privacy Regulations or
3. any other rights under the Privacy Regulations as a condition of Treatment or Payment Activities.

III. PROCEDURE:

1. Any person with knowledge of a violation of this Policy shall report the incident to the HIPAA Compliance Officer.
2. If the HIPAA Compliance Officer receives a report of a violation of this Policy, and will conduct an investigation to determine if a violation has occurred. If the report is substantiated, sanctions will be imposed pursuant to the Sanctions policy.

IV. REFERENCES:

1. AMC HIPAA Privacy Guidelines, PRIV. 56 (pg. 206).
2. HIPAA Privacy Regulations, 45 C.F. R. 164.530(h).
I. PURPOSE: To provide for training regarding PPMOK’s HIPAA Privacy Policies.

II. POLICY: PPMOK will provide training for all Personnel as to HIPAA and these Privacy Policies.

- PPMOK will annually train its workforce members regarding Privacy Policies and the manner in which such Policies relate to the members’ function within PPMOK.

- PPMOK will train each new member of its workforce as to compliance with the Privacy Policies.

- PPMOK will review and assess the sufficiency of its training protocols on an as-needed basis and provide additional training when and how indicated.

III. PROCEDURE: PPMOK, through the HIPAA Compliance Officer, will direct the methods and manner in which PPMOK’s Privacy training will be accomplished.

1. Training materials shall include a test or some other opportunity to demonstrate understanding of the information presented. Training must be completed according to the standards in this Policy in order for the training requirement to be satisfied.

2. It is the responsibility of PPMOK, in coordination with the HIPAA Compliance Officer, to ensure that its employees receive training according to its HIPAA Privacy Policies.

3. Training will be tracked with the assistance of the HIPAA Compliance Officer.

4. Each new employee must complete HIPAA Privacy training within 30 days of beginning work for PPMOK. The failure of an employee to complete the required training within 30 days after hire is grounds for Sanctions, up to and including termination or dismissal, unless good cause for the delay can be shown. (See, Sanctions.) Personnel shall ensure an adequate opportunity for training is provided to each new employee.
5. Each employee whose job functions are affected by a material change in PPMOK’s Privacy Policies will receive training regarding that material change within thirty (30) days after the change becomes effective. PPMOK or the HIPAA Compliance Officer (or designee) will provide such training.

6. Employees who fail to complete the training are subject to Sanctions pursuant to the Sanctions policy set forth herein.

7. Documentation regarding training must be maintained by HIPAA Compliance Officer, in written or electronic format, for at least six (6) years, or for as long as required by other applicable PPMOK policies.

8. If PPMOK encounters difficulty with individual employees complying with the training requirements, the supervisor should contact the HIPAA Compliance Officer.

IV. REFERENCES:

1. AMC HIPAA Privacy Guidelines, PRIV.50 (pg. 194-195)
2. HIPAA Privacy Regulations, 45 CFR §164.530.
I. PURPOSE: To establish minimum safeguards that must be implemented by PPMOK to protect the confidentiality PHI.

II. POLICY: PPMOK will implement appropriate administrative, technical, and physical safeguards that will reasonably safeguard PHI from intentional or unintentional Use or Disclosure in violation of its Privacy and Security Policies and the Privacy or Security Regulations and limit incidental Uses or Disclosures of PHI.

1. Personnel must reasonably safeguard PHI to limit incidental Uses or Disclosures made pursuant to an otherwise permitted or required Use or Disclosure.

2. PPMOK may not Disclose PHI without patient Authorization (unless otherwise permitted or Required by Law.) Personnel who perform services for PPMOK and any other Covered Entity must not otherwise Use or Disclose PHI created or received in the course of or incidental to their work for the PPMOK or any other Covered Entity and must use their best efforts to segregate the Use of the PHI.

3. This policy establishes minimum administrative and physical standards regarding the protection of PHI that PPMOK must enforce, as applicable. PPMOK may develop additional policies and procedures that are stricter than the parameters set forth in this Policy to address the unique circumstances of a particular situation. The development and implementation of policies and procedures in addition to those stated herein shall be reviewed by the HIPAA Compliance Officer for approval prior to implementation.

4. Technical safeguards regarding the protection of PHI maintained in electronic form are available from the HIPAA Compliance Officer. Some are incorporated into this Policy by reference.
III. PROCEDURE:

Administrative Safeguards:

1. **Oral Communications.** Personnel must exercise due care to avoid unnecessary Disclosures of PHI through oral communications. Voices should be modulated and attention should be paid to unauthorized listeners in order to avoid unnecessary Disclosures of PHI. Patient identifying information should not be Disclosed during oral conversations unless necessary to further Treatment, Payment, or Operational purposes. Dictation and telephone conversations must be conducted away from public areas if possible. Speakerphones may be used only in private areas.

2. **Telephone Messages.** Telephone messages and appointment reminders may be left on answering machines and voice mail systems, unless the patient has requested and received approval for an alternate means of communication pursuant to Communication by Alternative Means. However, Personnel shall limit the PHI that is Disclosed in a telephone message. Telephone messages regarding test results or that contain information that links a patient’s name to a particular medical condition must be avoided.

3. **Faxes.** The following procedures must be followed when faxing PHI: **Only the PHI necessary to meet the authorized requester’s needs may be faxed.**
   a. **PPMOK shall designate Personnel who can fax, or approve the faxing of, PHI. Unauthorized employees should not fax PHI.**
   b. Unless otherwise permitted or Required by Law, a properly completed and signed Authorization must be obtained before releasing PHI to third parties for purposes other than Treatment, Payment, or Health Care Operations as provided in Privacy-23, Authorization. PHI may be faxed to a number provided by an individual if the individual requests access to his/her own PHI via a completed Authorization form, in accordance with Patient Access to PHI.
   c. All faxes containing PHI must be accompanied by a cover sheet that includes a confidentiality notice. PHI may not be included on the cover sheet. A sample fax cover sheet is available on the HIPAA Forms webpage.
   d. Reasonable efforts should be made to verify that fax transmissions are sent to the correct destination. Frequently used numbers should be programmed into fax machines or computers to avoid dialing errors. Programmed numbers should be verified on a regular basis. The numbers of new recipients should be verified prior to transmission.
   e. Fax machines must be located in secure areas not readily accessible to visitors or patients. Incoming faxes containing PHI must not be left sitting on or near the machine for extended periods of time.
f. Fax confirmation sheets shall be reviewed to ensure the intended destination matches the number on the confirmation. The confirmation sheet shall be attached to the document that was faxed.
g. All instances of misdirected faxes containing PHI must be reported, investigated, and mitigated pursuant to Complaint Reporting and Tracking; Mitigation; and Accounting of Disclosures; as well as any internal reporting requirements.

4. **Mail.** PHI mailed outside PPMOK should be sent via first class mail, and the contents must be concealed. Appointment reminders may be mailed to a patient, unless the patient has requested and received approval for an alternative means of communication pursuant to Communication by Alternative Means.

5. **Copying.** All copies of PHI provided to the patient or another third party in response to a request for access should be date stamped in a color other than black or should bear some other unique identifying mark or symbol, so that a copy can be distinguished from the original.

6. Date stamping or marking records provided to patients will protect PPMOK in the event there is a dispute as to how certain records were acquired or Disclosed.

**Destruction Standards.** PHI must be discarded in a manner that protects the confidentiality of such information. Paper and other printed materials containing PHI shall be destroyed or cross-cut shredded so that it cannot be read or reconstructed.

At this time, PPMOK does not destroy electronic health records.

Magnetic media and diskettes containing PHI shall be overwitten, reformatted, or destroyed pursuant to PPMOK’s Electronic Data Disposal and Reuse policy.

**Physical Safeguards.**

1. **Paper Records.** Paper records and medical charts must be stored or filed in such a way as to avoid access by unauthorized persons. Some type of physical barrier must be used to protect paper records from unauthorized access. Paper records and medical charts on desks, counters, or nurses’ stations must be placed face down or concealed to avoid access by unauthorized persons. Paper records shall be secured when the office area is unattended by persons authorized to have access to paper records.
   a. Paper records stored outside of PPMOK must be inventoried and stored in a secure facility. PPMOK shall maintain a log of who has access to the stored records and have in place a procedure for terminating access when employment ends.
   b. PPMOK employees shall not remove paper records or medical charts for their own convenience. Original paper records and medical charts may not be removed from PPMOK premises unless necessary to provide care or Treatment to a patient or Required by Law. Any paper records and medical charts that must be removed
from PPMOK premises shall be checked out according to any applicable PPMOK policies and procedures and must be returned as quickly as possible. The safety and return of the medical records checked out or removed are the sole responsibility of the person who checked them out or removed them.

c. Paper records and medical charts that are removed from PPMOK premises must not be left unattended in places in which unauthorized persons can gain access, legally or otherwise. Paper records and medical charts should not be left in automobiles or in view of passers-by.

d. The theft or loss of any paper record or medical chart shall be reported immediately to the HIPAA Compliance Officer and any person designated by the PPMOK so that mitigation options can be considered and implemented as soon as possible.

2. **Escorting Visitors and Patients.** Visitors and patients must be appropriately escorted and monitored when on PPMOK premises where PHI is located to ensure they do not have access to PHI about other patients. PPMOK shall not permit unescorted visitors or patients in areas containing PHI.
   
   a. Persons who are not employed by PPMOK, including but not limited to pharmaceutical representatives and device salespeople, shall not be in areas in which patients are being seen or treated or where PHI is stored, without appropriate continuous supervision.

3. **Computer/Work Stations.** Computer monitors must be positioned away from common areas, or a privacy screen must be installed to prevent unauthorized access to or observation of PHI. The screens on unattended computers must be returned to a password-protected screen saver or login screen. The workstation shall be set to log out any user after forty-five (45) minutes of inactivity.

**Technical Safeguards.** Telemedicine Technology. The use of Telemedicine Technology must meet all Safeguards as specified in the HIPAA Privacy and Security Policies and AES Encryption standards for H.323 protocol communications. Contact the HIPAA Compliance Officer for additional information.

1. E-mail within PPMOK. Sending e-mails within the PPMOK e-mail system that contain PHI for Treatment, Payment, or Health Care Operations is acceptable. PHI sent should be limited to the minimum necessary and should be sent as a limited data set when possible.

2. E-mail outside PPMOK. Except in emergency situations, the use of e-mail to transmit PHI outside PPMOK for Treatment, Payment, or Health Care Operations is prohibited unless the message is encrypted between sender and recipient in a manner that satisfies HITECH requirements.

3. All e-mails containing PHI transmitted by PPMOK or its representatives must contain a Confidentiality Notice similar to the following: **Confidentiality Notice** “This e-mail,
including any attachments, contains information that may be confidential or privileged. The information is intended to be for the use of the individual or entity named above. If you are not the intended recipient, be aware that any disclosure, copying, distribution, or use of the contents is prohibited. If you have received this e-mail in error, please notify the sender immediately by a “reply to sender only” message and destroy all electronic and hard copies of the communication, including attachments.”

4. Without Encryption Capabilities (E-Mail Communication Denial). If a patient sends an e-mail to an employee asking a health care question or requesting any type of information that would require a Disclosure of PHI, the request for response shall be declined by sending a message similar to the following:
   a. “I have received your health care question or request for health information. However, I cannot respond using e-mail because to do so would require the transmission of information that I consider to be highly sensitive, and e-mails can be intercepted easily. I will respond to your question or request through some other means of communication. If you wish to receive health information via email, please submit Consent for Electronic Communication form to your health care provider.”

5. When e-mail Encryption is Available, Personnel may send PHI via email only if:
   a. The patient has submitted a complete Consent for Electronic Communication Form\(^\text{11}\)
   b. The email will be included in the patient’s medical record when appropriate.
   c. The PHI will be sent, maintained, and accessed in compliance with PPMOK HIPAA policies and any other relevant procedures.
   d. The employee must comply with PPMOK Privacy Policies regarding accounting of disclosures.

6. Electronic Documents. Documents and attachments and/or images containing PHI must be stored on network servers with appropriate security restrictions.

7. Portable Computing Devices (e.g., laptops and hand-held computers). Employees must use extreme caution when using Portable Computing Devices to store PHI. PHI should not be stored on Portable Computing Devices unless absolutely necessary but rather should be stored on servers in a secure enterprise data center. Portable Computing Devices must never be left unattended in unsecured places.
   a. Those storing PHI on personal portable devices are responsible for the security of the PHI stored on such devices. PHI contained on such devices must be encrypted pursuant to PPMOK’s Portable Computing Device Security Policy and Standard. All PPMOK Standards for Portable Computing Device Security, such

\(^{11}\) Note: The Consent for Electronic Communication form is available on the PPMOK webpage.
as password protection, must be followed. The failure to take appropriate security precautions will be considered a violation of these Policies subjecting the user to sanctions.

8. Other Uses of the Internet. Any other electronic transmission of PHI requires that appropriate safeguards and procedures be implemented and approved by the HIPAA Compliance Officer.

9. **Use of Social Media Sites.** PHI shall not be posted on social media sites, such as Facebook or Twitter. Personnel should keep in mind that even if a patient’s name is not posted, in the event the patient could reasonably be identified by the information posted, the information is considered PHI. Therefore, information regarding patients should not be posted on social media sites.

10. Use of Digital Copiers/Scanners. PPMOK Personnel using digital copiers, scanners, and fax machines must verify that appropriate data security features (e.g., encryption, overwriting) are enabled. In addition, before such equipment is returned to the vendor, considered surplus, or otherwise disposed of, PPMOK must take steps to ensure the hard drive is destroyed or completely overwritten. These steps may include, but are not limited to, imposing these requirements on the vendor or working with IT.

11. Theft or Loss. The theft or loss of any electronic medical record or device containing PHI (including those owned by the individual) shall be reported immediately to the HIPAA Compliance Officer, as appropriate, and any person designated by PPMOK so that mitigation and reporting options can be considered and implemented as soon as possible. See Security Breaches.

**IV. REFERENCES:**

1. AMC HIPAA Privacy Guidelines, PRIV. 510 (pg. 196-197).
2. HIPAA Privacy Regulations, 45 CFR §164.530.
I. PURPOSE: To establish a process for imposing sanctions in the event PPMOK’s Privacy Policies or the Privacy Regulations are violated.

II. POLICY: PPMOK will apply sanctions as appropriate against Personnel and its Business Associates who fail to comply with PPMOK’s Privacy Policies and/or the Privacy Regulations.

PPMOK will not impose sanctions against Personnel or Business Associates for:

1. engaging in good faith whistleblower activities related to Privacy issues;
2. submitting a complaint in good faith to the Secretary of the Department of Health and Human Services or other enforcement agency;
3. participating in an investigation regarding Privacy issues; or
4. appropriately registering opposition to a violation of the Privacy Policies or Regulations.

III. PROCEDURE:

Employees. A violation of PPMOK’s Privacy Policies or Regulations by an employee will also be considered a violation of PPMOK’s Employment Manual (the “Manual”). The sanctions set forth in the Manual apply equally to violations of PPMOK’s Privacy Policies. The sanction imposed for a violation of the Privacy Policies depends on the severity of the violation and will be imposed in accordance with the Manual.

Business Associates. If PPMOK identifies or determines a pattern of activity or practice of a Business Associate that constitutes a material breach or violation of the Business Associate’s obligations under his/her/its contract with PPMOK or the Privacy Regulations, PPMOK will take reasonable steps to cure the breach or end the violation, as applicable, and, if such steps are unsuccessful or not appropriate, shall:

1. terminate the contract, if feasible; or
2. report the problem to the Secretary of the Department of Health and Human Services or other applicable enforcement agency.

**Documentation.** Documentation regarding any sanction imposed for a violation of the Privacy Policies or Privacy Regulations shall be retained in the sanctioned person’s personnel file in written or electronic format, for at least six (6) years. Copies of such documentation should be forwarded to the HIPAA Compliance Officer upon request, who also should maintain such documentation for the minimum retention period. Documentation of any sanction imposed against a Business Associate should be retained by the HIPAA Compliance Officer for the minimum retention period. Documentation as to any Business Associate shall be retained by the HIPAA Compliance Officer in written or electronic format for at least six (6) years.

**Sanctions.** When imposing sanctions for the inappropriate Use and Disclosure of PHI, consideration should be given to issues such as whether the Use or Disclosure was made as a result of:

1. carelessness or negligence,
2. curiosity, or
3. the desire for personal gain or malice.

**IV. REFERENCES:**

1. AMC HIPAA Privacy Guidelines, PRIV. 53 (pg. 200-201).
2. HIPAA Privacy Regulations, 45 C.F. R. 164.530(e).
I. PURPOSE: To outline required and permitted Uses and Disclosures of PHI.

II. POLICY: PPMOK shall not Use or Disclose PHI except as permitted by its Privacy Policies and the Privacy Regulations.

Required Disclosures: PPMOK will Use or Disclose PHI:

1. to a patient, when requested under, and as required by Privacy-05, Patient Access to Protected Health Information; and Privacy-06, Accounting of Disclosures; and

2. when required by the Secretary of the Department of Health and Human Services to investigate PPMOK’s compliance with the Privacy Regulations or

3. otherwise Required by Law.

III. PROCEDURE:

Permitted Uses and Disclosures: PPMOK and PPMOK Personnel are permitted to Use or Disclose Protected Health Information as follows:

1. for Treatment, Payment, or Health Care Operations, as permitted by and in compliance with Privacy-22, Treatment, Payment, and Health Care Operations:

2. incident to a Use or Disclosure otherwise permitted or required by the Privacy Regulations as long as the Minimum Necessary (Privacy-21) and Safeguard (Privacy-18) policies have been followed;

3. pursuant to an Authorization as permitted by Privacy-23, Authorization, and Privacy-28, Marketing;
4. pursuant to an agreement under, or as otherwise permitted by, Privacy-26, Disclosures to Family and Others Involved in Patient’s Care, and Privacy-33, Facility Directory; and as permitted by and in compliance with Privacy-24, Mental Health Records; Privacy-25, Required by Law; Privacy-27, Business Associate; Privacy-29, Fundraising; Privacy-30, Research; and Privacy-31, Limited Data Set.

5. to report unlawful or unprofessional conduct or conduct that endangers others that a whistleblower believes in good faith PPMOK has engaged in, so long as the Disclosure is to a Health Oversight Agency/Public Health Authority or health care accreditation organization that has authority to investigate such conduct or an attorney retained to advise the reporting party on legal options.

6. by any Personnel who is the victim of a crime reporting to Law Enforcement, so long as the PHI disclosed is about the suspect and is limited name and address, date and place of birth, SSN, ABO blood type and rh factor, type of injury, date and time of treatment, date and time of death if applicable, and distinguishing physical characteristics.

7. certain immunization records without the standard Authorization form to a school about an individual who is a student or prospective student of the school, or to the individual, if the requested information is for presentation to a school and if:
   a. the PHI that is disclosed is limited to proof of immunization; and
   b. the school is required by state or other law to have such proof of immunization prior to admitting the individual; and
   c. PPMOK obtains and documents the request for the disclosure from either
      i. a parent, guardian, or other person acting in loco parentis of the individual, if the individual is not an emancipated minor; or
      ii. the individual, if the individual is an adult or emancipated minor.

8. PPMOK may accept on a verbal request if it documents the request. All requests must be documented.

9. For other Uses and Disclosures, Personnel should consult with the Compliance Officer.

IV. REFERENCES:

1. 45 C.F. R. § 164.502
2. 45 C.F.R. § 164.512
**I. PURPOSE:** To describe the application of the minimum necessary rule as it relates to Uses and Disclosures of and requests for PHI.

**II. POLICY:** Personnel must make reasonable efforts to limit the Use and Disclosure of and requests for PHI to the minimum that is reasonably necessary to accomplish the intended purpose of the Use, Disclosure, or request.

**The minimum necessary rule does not apply to:**

1. Disclosures to or requests by a Health Care Provider for Treatment;

2. Disclosures to the patient or his/her legal representative (See Personal Representatives; and Patient Access to Protected Health Information);

3. Uses or Disclosures made pursuant to an Authorization (See Authorization);

4. Disclosures made to the Secretary of the Department of Health and Human Services for compliance and enforcement of the Privacy Regulations (See Uses and Disclosures);

5. Uses and Disclosures Required by Law (See Required by Law, except as otherwise stated in each subsection);

6. Uses and Disclosures required for compliance with HIPAA standardized transactions.

**III. PROCEDURE:** Personnel shall not Use, Disclose, or request an entire medical record, except when the entire medical record is specifically justified as that which is reasonably necessary to accomplish the purpose for the Use, Disclosure, or request.
1. PPMOK must designate Personnel who need access to PHI to carry out their duties and must designate the level of access needed and the conditions appropriate to such access. Access descriptions shall be incorporated in job descriptions for each employee position.

2. A Role-Based Access Worksheet must be completed for each employee. PPMOK shall be responsible for completing the Worksheet upon the employee’s initial placement and, as applicable, when the employee’s responsibilities change. A copy of the Worksheet for employees must be sent to Human Resources for inclusion in the employee’s file. The original is maintained by PPMOK.

3. Personnel who are directly involved in a patient’s Treatment and care (e.g., physicians and nurses) may have access to the patient’s entire PHI. Personnel who are not directly involved in a patient’s Treatment shall not have unlimited access to a patient’s PHI.

4. It is a violation of the minimum necessary rule for a Health Care Provider to access the PHI of patients with whom the provider has no Treatment relationship, unless otherwise permitted by the Privacy Regulations and these Policies.

Disclosures

1. Routine Disclosures: PPMOK shall implement standard protocols, when appropriate, to limit the PHI Disclosed on a routine or recurring basis. Copies of such protocols shall be maintained by PPMOK and provided to the HIPAA Compliance Officer upon request.

2. Non-Routine Disclosures: All non-routine Disclosures (those that do not occur on a day-to-day basis as part of Treatment, Payment, or Health Care Operation activities or which are Required by Law on a regular basis) must be made in writing and submitted to the HIPAA Compliance Officer. When considering non-routine Disclosures, consideration should be given to the following criteria:
   a. the purpose of the request;
   b. any potential harm that would result to the patient, PPMOK, or any other third party as a result of the Disclosure;
   c. the relevance of the information requested; and
   d. other applicable state and federal laws and regulations.

3. Personnel may rely, if such reliance is reasonable under the circumstances, on a requested Disclosure as the minimum necessary for the stated purpose when:
   a. making Disclosures to public officials as Required by Law, if the public official represents that the information requested is the minimum necessary for the stated purpose;
   b. the information is requested by another Covered Entity; or
c. the information is requested by a professional who is an employee of PPMOK or is a Business Associate of PPMOK providing professional services, if the employee or Business Associate represents that the information is the minimum necessary for the stated purpose(s).

Requests

1. **Routine Requests** PPMOK shall implement standard protocols, when appropriate, to limit the PHI requested on a routine or recurring basis. Copies of such protocols should be maintained by PPMOK and provided to the HIPAA Compliance Officer upon request.

2. **Non-Routine Requests**: PPMOK shall all non-routine requests (those that do not occur on a day-to-day basis as part of Treatment, Payment or Health Care Operation activities) to the HIPAA Compliance Officer for review. When considering non-routine requests, the following criteria must be considered:
   a. the reason for the request;
   b. any potential harm that would result to the patient, PPMOK, or any other third party as a result of the Disclosure;
   c. the relevancy of the information requested; and
   d. other applicable state and federal laws and regulations.

IV. REFERENCES:

1. AMC HIPAA Privacy Guidelines, PRIV. 39 (pg. 154).
2. HIPAA Privacy Regulations, 45 CFR 164.502(b); 45 CFR 164.514(d).
I. PURPOSE: To establish permitted Uses and Disclosures of PHI for Treatment, Payment, and Health Care Operations.

II. POLICY: PPMOK may Use or Disclose PHI for its own Treatment, Payment, or Health Care Operations. PPMOK may also disclose PHI:

1. for Treatment activities of another Health Care Provider;

2. to another Covered Entity or a Health Care Provider for the Payment activities of the entity that receives the information; and

3. to another Covered Entity for certain enumerated Health Care Operations activities of the entity that receives the information, if each entity either has or had a relationship with the patient who is the subject of the PHI being requested and the health information pertains to such relationship.

4. PHI can be exchanged between two Covered Entities for the following Health Care Operations:
   a. conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities;
   b. population-based activities relating to improving health or reducing health care costs;
   c. protocol development,
   d. case management and care coordination;
   e. contacting Health Care Providers and patients with information about Treatment alternatives;
f. reviewing the competence or qualifications of Health Care Professionals;
g. evaluating practitioner and provider performance;
h. conducting training programs in which trainees or practitioners in areas of health care learn under supervision to practice or improve their skills as Health Care Providers;
i. training non-health care professionals; and
j. accreditation, certification, licensing, or credentialing activities.

5. To the extent, PPMOK participates in an organized health care arrangement, it may disclose PHI about an individual to another Covered Entity that participates in the Organized Health Care Arrangement for any Health Care Operations activities of the Organized Health Care Arrangement.

6. Uses and Disclosures of a patient’s PHI other than for Treatment, Payment, and Health Care Operations of PPMOK or another Health Care Provider, PPMOK must obtain an Authorization from the patient pursuant to the Authorization policy, unless Disclosure pursuant to another Policy is permitted and/or required. (Contact the HIPAA Compliance Officer for assistance.)

7. A patient Authorization is required for exchanges of PHI between PPMOK and any other Covered Entity, unless the exchange is specifically permitted under the Privacy Regulations.

III. REFERENCES:

1. HIPAA Privacy Regulations, 45 C.F.R. 164.506
2. FERPA, 20 USC 1232g; 34 C.F.R. Part 99.
Authorization

Subject: Authorization Page: 1 of 2

Policy #: Privacy-24 (Uses & Disclosures) Approved: April 16, 2014

Effective Date: April 16, 2014 Revised:

Next Review Date: June 30, 2014 Reviewer:

I. PURPOSE: To establish Authorization requirements for Uses and Disclosures of PHI other than for Treatment, Payment, and Health Care Operations.

II. POLICY: PPMOK shall not Use or Disclose PHI for purposes other than Treatment, Payment, and Health Care Operations without a valid written Authorization from the patient, except as otherwise permitted by these Policies. When PPMOK obtains or receives a valid Authorization for Use or Disclosure of Protected Health Information, such Use or Disclosure must be consistent with the Authorization.

1. Information released pursuant to Authorization may include alcohol and/or drug abuse records protected under federal and/or state law. Re-disclosure of such alcohol and/or drug abuse records by the identified recipient is prohibited without specific Authorization.

2. An Authorization is required to disclose information to third parties for purposes other than Treatment, Payment, or Health Care Operations and for Use by or Disclosures to any other person or entity.


4. Marketing PPMOK must obtain an Authorization for any Use or Disclosure of Protected Health Information for marketing, except in certain circumstances. See, Marketing policy.

5. Conditioning of Authorizations Generally, PPMOK may not condition the provision of Treatment to a patient on the receipt of an Authorization.
a. One exception to the prohibition on conditioning Treatment on the receipt of Authorization relates to health care services provided at the request of a third party. For example, PPMOK can require an Authorization as a condition to providing a drug screening test or physical requested by an employer.

6. Revocation of Authorizations: PPMOK must permit patients to revoke their Authorizations, except to the extent it has already taken action in reliance on the Authorization. To revoke an Authorization, a patient must provide written notice to PPMOK.

III. PROCEDURE:

1. Any individual desiring access to or a copy of his PHI must submit a valid Authorization to PPMOK. The Authorization must contain all of the elements required by the Privacy Regulations and State law.

2. Prior to using or disclosing PHI pursuant to an Authorization, Personnel shall review the Authorization to determine if it is valid. Personnel may contact the HIPAA Compliance Officer for help in determining whether an Authorization is valid. An Authorization is not valid if it contains any of the following defects:
   a. the expiration date has passed or the expiration event is known to have occurred;
   b. the Authorization has not been filled out completely;
   c. Personnel have knowledge that the Authorization has been revoked;
   d. Personnel have knowledge that some material information in the Authorization is false;
   e. the Authorization was obtained by improperly conditioning Treatment upon its receipt;
   f. the Authorization is missing one of the elements required by the Privacy Regulations or State law; or
   g. if the Authorization is for Psychotherapy Notes and is combined with another type of Authorization or document.

3. If PPMOK seeks an Authorization from a patient for a Use or Disclosure of Protected Health Information, PPMOK must provide the patient with a copy of the signed Authorization.

4. PPMOK must keep copies of Authorizations in the patient file for at least six (6) years.

IV. REFERENCES:

1. AMC HIPAA Privacy Guidelines, PRIV. 10 (pg. 90).
2. HIPAA Privacy Regulations, 45 C.F.R. 164.508
I. PURPOSE: To establish permitted uses and Disclosures of mental health records, including Psychotherapy Notes.

II. POLICY: A patient generally has the right to access his/her mental health records other than Psychotherapy Notes. A patient can be denied access to his/her mental health records for one of the reasons set forth in the Patient Access to Protected Health Information policy.

1. Mental health records, other than Psychotherapy Notes, may be Used and Disclosed by Personnel for Treatment, Payment, and Health Care Operations to the same extent, and subject to the same limitations, applicable to other types of PHI as set forth in these Policies and in accordance with applicable mental health statutes.

2. Persons or entities who desire access to a patient’s mental health records for purposes other than Treatment, Payment, or Health Care Operations must obtain an Authorization as required by the Authorization policy unless otherwise permitted by these Policies. The HIPAA Compliance Officer should be contacted for assistance with mental health record requests.

3. An Authorization for the Use or Disclosure of Psychotherapy Notes cannot be combined with Authorization for release of other medical records.

Remember: Psychotherapy Notes have a very limited definition. They 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.
4. **Psychotherapy Notes** A patient does not have a right to access Psychotherapy Notes relating to him/herself unless (i) the patient’s Treatment professional approves such access in writing; or (ii) the patient obtains a court order authorizing such access.
   a. A patient Authorization must be obtained for any Use or Disclosure of Psychotherapy Notes, except for the following purposes:
   b. Use by the originator (the creator) of the Psychotherapy Notes for Treatment purposes;
   c. Use or Disclosure of Psychotherapy Notes by Personnel for conducting training programs in which trainees or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family, or individual counseling;
   d. Use or Disclosure to legal counsel or designee to defend PPMOK in a legal action or other proceeding brought by the patient;
   e. Use or Disclosure to the Secretary of Health and Human Services, or any other officer or employee of the Department of Health and Human Services to whom the authority has been delegated, to conduct enforcement activities;
   f. Use or Disclosure needed for oversight of Personnel who created the Psychotherapy Notes;
   g. Use or Disclosure needed by a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or conducting other duties as authorized by law; or
   h. When Personnel, in good faith, believe the Use or Disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public.
   i. The Privacy Regulations do not permit a health plan to condition enrollment, eligibility for benefits, or payment of a claim on obtaining a patient’s Authorization to Use or Disclose Psychotherapy Notes.

**III. REFERENCES:**

1. HIPAA Privacy Regulations, 45 CFR § 164.508(b)(3)(ii) and § 164.524(a).
I. PURPOSE: To set forth standards regarding Uses and Disclosures of PHI Required by Law.

II. POLICY: Personnel may Disclose PHI without the patient’s consent, Authorization, or opportunity to agree or object as required by applicable state and federal laws. Relevant laws include, but are not limited to the following:

Questions regarding whether a particular Use or Disclosure is Required by Law must be submitted to the HIPAA Compliance Officer.

III. PROCEDURE:

Abuse or Neglect of Children.

1. Reporting Child Abuse, Neglect, or the Birth of a Chemically-Dependent Child. All Personnel who have reason to believe that a child under the age of 18 is a victim of abuse or neglect or who attend the birth of a child who tests positive for alcohol or a controlled dangerous substance must promptly notify the Oklahoma Department of Human Services. PPMOK notes that attendance at the birth of children is unlikely to occur in PPMOK. PPMOK should establish procedures for facilitating and coordinating reporting requirements.

2. “Abuse” for purposes of this section means harm or threatened harm to the child’s health, safety, or welfare by a parent; legal guardian; custodian; foster parent; adult residing in the home of the child; the owner, operator, or employee of a child care facility; or an agent or employee of a private residential home, institution, facility, or day treatment program.

3. “Neglect” for purposes of this section means (i) failure to provide adequate food, clothing, shelter, medical care, and supervision; (ii) failure to provide special care which
is necessary because of the physical or mental condition of the child; or (iii) abandonment.

4. Reports of abuse or neglect shall be made to the telephone hotline established by DHS. The state hotline to report abuse is: 1(800) 522-3511

A written record of each such report and the circumstances surrounding such report shall be maintained by PPMOK making the report. The report must contain the following:

   a. The names and addresses of the child and the child’s parents or other persons responsible for the child’s health, safety, or welfare;
   b. The child’s age;
   c. The nature and extent of the abuse or neglect, including any evidence of previous injuries;
   d. Whether the child has tested positive for alcohol or a controlled dangerous substance; and
   e. Any other information that may be helpful in establishing the cause of the injuries and the person or persons responsible.

5. PPMOK must also provide copies of the results of the examination or copies of the examination on which the report was based and any other clinical notes, x-rays, photographs, and other previous or current records relevant to the case to Law Enforcement officers conducting a criminal investigation into the case and to employees of the Department of Human Services conducting an investigation of alleged abuse or neglect in the case, upon written verification by the applicable agency of a pending investigation.

   a. Reporting Criminally Inflicted Injuries. Personnel examining, attending, or treating a child suffering from what appears to be criminally injurious conduct, including, but not limited to, a misdemeanor or felony that results in bodily injury, threat of bodily injury, or death, or child physical or sexual abuse shall promptly report the matter to the Department of Human Services by calling the child abuse hotline, and to the local police department.

   i. The report may require the disclosure of PHI relevant to the investigation. PPMOK should only release the minimum amount of information necessary to adequately report the abuse.

6. Notification. To the extent a report is made pursuant to 1 (a) or (b) above, Personnel must promptly notify the Personal Representative of the child who is the subject of the report, unless Personnel, in the exercise of professional judgment, believe informing the Personal Representative would place him/her at risk of serious harm or if they believe

13 The state hotline to report abuse is: 1(800) 522-3511
14 Verification forms are available on the web site and from the HIPAA Compliance Officer.
such Personal Representative is responsible for the abuse, neglect, or other injury and that informing such person would not be in the best interests of the child.

**Abuse of Vulnerable Adults** Personnel who have reasonable cause to believe that a Vulnerable Adult is suffering from abuse, neglect, or exploitation shall promptly report the matter to the Oklahoma Department of Human Services\(^\text{15}\) and the local police or sheriff’s department.

1. **Definitions:**
   a. “Vulnerable Adult” is a patient who is incapacitated or who, because of physical or mental disability, incapacity, or other disability, is substantially impaired in the ability to provide adequately for the care or custody of him/herself; is unable to manage his or her property and financial affairs effectively; is unable to meet essential requirements for mental or physical health or safety; or is unable to protect him/herself from abuse, neglect, or exploitation without assistance from others.
   b. “Abuse” for purposes of this section means causing or permitting: (i) the infliction of physical pain, injury, sexual abuse, sexual exploitation, unreasonable restraint or confinement, or mental anguish, or (ii) the deprivation of nutrition, clothing, shelter, health care, or other care or services without which serious physical or mental injury is likely to occur to a Vulnerable Adult by a caretaker or other person providing services to a Vulnerable Adult.
   c. “Exploitation” or “Exploit” means an unjust or improper use of the resources of a Vulnerable Adult for the profit or advantage, economic or otherwise, of a person other than the Vulnerable Adult through the use of undue influence, coercion, harassment, duress, deception, false presentation, or false pretense.
   d. “Neglect” for purposes of this section means: (i) the failure to provide protection for a Vulnerable Adult who is unable to protect his or her own interest; (ii) the failure to provide a Vulnerable Adult with adequate shelter, nutrition, health care, or clothing; or (iii) the causing or permitting of harm or the risk of harm to a Vulnerable Adult through the action, inaction, or lack of supervision by a caretaker providing direct services.

2. **Reports** PPMOK shall provide PHI to Law Enforcement officers or employees conducting investigations upon written verification\(^\text{16}\) by the applicable agency of a pending investigation. Reports regarding victims of Abuse, Neglect, or domestic violence, must contain:
   a. the name and address of the Vulnerable Adult,
   b. the name and address of the caretaker, if any, and

---

\(^{15}\) The state hotline to report abuse is 1 (800) 522-3511
\(^{16}\) Verification forms are available on the web site and from the HIPAA Compliance Officer.
c. a description of the current location and current condition of the Vulnerable Adult
d. a description of the situation which may constitute Abuse, Neglect, or Exploitation of the Vulnerable Adult.

3. Reporting Criminally-Injurious Conduct. Any Personnel examining, attending, or treating a patient for what appears to be criminally-injurious conduct, including, but not limited to, a misdemeanor or felony that results in bodily injury, threat of bodily injury, or death, shall promptly report the matter to the Department of Human Services and the local police department. The report may require the disclosure of PHI relevant to the investigation. PPMOK should release only the minimum amount of PHI needed to adequately report the abuse.

4. Notification. To the extent a report is made pursuant to 2 (a) or (b) above, Personnel must promptly notify the Personal Representative of the Vulnerable Adult who is the subject of the report, unless Personnel, in the exercise of professional judgment, believe informing the individual would place him/her at risk of serious harm if they believe that such Personal Representative is responsible for the abuse, neglect, or other injury, and that informing such person would not be in the best interests of the Vulnerable Adult.

Judicial and Administration Procedure

1. Definitions:
   a. Court Orders: A written direction of the court, filed of record with a court having jurisdiction over PPMOK, and signed by a judge.
   b. Subpoena: A subpoena is a unilateral request of a party for the production of documents. A subpoena is not generally approved by a judge, and in some circumstances may be signed by a private attorney.
      i. Note: it is important for PPMOK to determine whether the patient’s Authorization or a court order is required for the release. All subpoenas must be sent to the HIPAA Compliance Officer, who shall review the subpoena and applicable laws and regulations before making a determination regarding release of information.

2. Procedure--Court Orders: Upon the receipt of a Court Order for the disclosure of medical records containing PHI,
   a. the recipient of the Order must immediately forward the Order to the HIPAA Compliance Officer’s office.
   b. Upon determining that the Order is valid and meets all legal requirements, Personnel will be advised to release the information pursuant to the court order. The patient whose records are being requested is not required to provide an Authorization for the Disclosure of the records pursuant to a court order.
c. **Special Requirements for Court Orders Relating to Substance Abuse Records.** Records of the identity, diagnosis, prognosis, or treatment of patients maintained in connection with substance abuse education, prevention, training, treatment, rehabilitation, or Research conducted, regulated by, or assisted by any United States department or agency shall be confidential, in accordance with State law.

i. **Disclosure of Substance Abuse Records.** The content of these records may be Disclosed to third parties as follows:
   1. in accordance with the patient’s prior written Authorization;
   2. to medical personnel to the extent necessary to meet a bona fide medical emergency;
   3. to qualified personnel for the purpose of conducting scientific Research, management audits, financial audits, or program evaluation only if the patient is not identified directly or indirectly;
   4. upon receipt of a valid court order that meets all of the requirements of 42 C.F.R. Part 2.

3. **Procedure—Subpoenas:** Upon receipt of a subpoena, the recipient of the subpoena must immediately forward the subpoena to the HIPAA Compliance Officer, who shall review the document, and applicable laws and regulations for a determination of whether PHI can be released pursuant to the subpoena.

**Disclosures for Law Enforcement Purposes.** Locate an Individual. Certain limited PHI regarding a patient may be Disclosed to a Law Enforcement Official who requests such information to identify or locate a suspect, fugitive, material witness, or missing person. Absent a request, such information may not be disclosed. A request may be made orally or in writing and may include a general request seeking the public’s assistance in identifying a suspect, fugitive, material witness, or missing person.

   1. If a request is made by a Law Enforcement Official for a patient’s PHI, the HIPAA Compliance Officer shall be contacted immediately to authenticate the request for disclosure and to determine whether the official is authorized to make such a request.

   2. Upon determining that the request is valid, the HIPAA Compliance Officer shall direct the appropriate person(s) to provide the limited information set forth below. The disclosure of PHI pursuant to this section is limited to the following:
      a. Name and address
      b. Date and place of birth
      c. Social Security Number
      d. ABO, blood type, and rh factor
      e. Type of injury, if applicable
      f. Date and time of treatment
g. Date and time of death, if applicable
h. A description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair, scars, and tattoos.

3. **Personnel should not disclose any of the following information:** DNA data and analyses, dental records, or typing samples or analyses of tissues or bodily fluids other than blood.

**Administrative Requests.** PPMOK may disclose PHI to Law Enforcement Officials pursuant to an administrative request (including an administrative subpoena or summons, a civil or an authorized investigative demand, or similar process authorized by Federal or State law), so long as:

1. the information sought is relevant and material to a legitimate Law Enforcement inquiry;
2. the request is specific and limited in scope to the extent reasonably practicable for the purpose; and
3. de-identified information cannot reasonably be used. Personnel should consult with the HIPAA Compliance Officer before making any Disclosures pursuant to this provision.

**Patient Crime Victim.** In addition to other Disclosures regarding potential victims of a crime, PPMOK may disclose to Law Enforcement Officials information about a patient who is suspected to be a victim of a crime, if:

1. the patient consents to the Disclosure; or
2. if the patient is unable to provide consent, all of the following requirements are met:

3. the Law Enforcement Officers provides PPMOK with written verification;
4. the Law Enforcement Official represents that such information is needed to determine whether a violation of law by a person other than the patient has occurred,
5. that such information is not intended to be used against the patient, and

---

17 Verification forms are available the web site forms page and from the HIPAA Compliance Officer. Personnel should consult with the HIPAA Compliance Officer before making any Disclosures pursuant to this provision.
6. that immediate Law Enforcement activity that depends on the Disclosure would be materially and adversely affected by waiting until the patient is able to consent; and

7. the Disclosure is in the best interest of the patient, as determined by Personnel in the exercise of professional judgment.

**Crime on Premises.** Personnel may Disclose to Law Enforcement Officials PHI which they believe in good faith constitutes evidence of criminal conduct occurring on PPMOK property. Personnel should consult with the Compliance Officer before making any Disclosures.

**Off-Premises Emergency.** Personnel providing emergency health care in response to a medical emergency, other than an emergency on PPMOK property, may Disclose PHI to a Law Enforcement Official if

1. the Disclosure appears necessary to alert Law Enforcement to:

2. the commission and nature of a crime;

3. the location of such crime or that of the victim(s) of such crime; and

4. the identity, description, and location of the perpetrator of such crime.

5. Personnel should consult with the HIPAA Compliance Officer before making any Disclosures pursuant to this provision.

**Uses or Disclosures to Avert Serious Threats to Health and Safety.** PPMOK may, consistent with applicable law and ethical standards, Use or Disclose PHI if Personnel, in good faith, believe such Use and Disclosure

1. is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public; and

2. the Disclosure is to a person or persons reasonably able to prevent or lessen the threat, including the target of the threat; or

3. is necessary for Law Enforcement Officials to identify or apprehend an individual who has made a statement admitting participation in a violent crime that Personnel reasonably believe may have caused serious physical harm to the victim

   a. (provided that no Disclosure may be made under this circumstance if the Disclosure is made during the course of Treatment to affect the propensity to commit the criminal conduct that is the basis for the Disclosure, or actual
counseling or therapy, or if the Disclosure is made during a request to initiate such Treatment); or
b. escaped from a Correctional Institution or from lawful custody. The HIPAA Compliance Officer should be consulted before any Disclosures of PHI are made pursuant to this provision.

**Uses and Disclosures for Specialized Government Functions.**

1. **Military.** PPMOK may Use and Disclose PHI of patients in the United States and foreign armed forces for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission. The HIPAA Compliance Officer should be consulted to confirm that the requirements of such Use or Disclosure are met.

2. **National Security.** PPMOK may Disclose PHI to authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities authorized by the National Security Act, and to protect the President of the United States and certain other public officials as authorized by law. The HIPAA Compliance Officer should be consulted to confirm that the requirements of this Disclosure are met.

3. **Correctional Institutes/Inmates.** PPMOK may Disclose to a Correctional Institution or Law Enforcement Official having lawful custody of an inmate or other individual, if the Correctional Institution or such Law Enforcement Official represents that such PHI is necessary for:
   a. the provision of Health Care to such individuals;
   b. the health and safety of such individual or other inmates;
   c. the health and safety of the officers or employees of or others at the Correctional Institution or other persons responsible for the transporting of inmates;
   d. Law Enforcement on the premises of the Correctional Institution; and/or
   e. the administration and maintenance of the safety, security, and good order of the Correctional Institution.
   f. The HIPAA Compliance Officer should be consulted to confirm that the requirements of this Disclosure are met.

**Public Health.**

1. PPMOK may Disclose PHI, without the written Authorization of the patient, to the appropriate state or federal health authority authorized by law to collect or receive such information for the purpose
   a. of preventing or controlling disease, injury, or disability;
   b. to conduct public health surveillance,
   c. public health investigations, or
d. public health interventions; or,

(e) at the direction of a Public Health Authority, to certain foreign governments;

(f) to a Public Health Authority authorized by law to receive reports of child abuse or neglect;

(g) to certain persons subject to FDA jurisdiction for limited purposes;

(h) to persons who may have been exposed to a communicable disease or may be at risk of such, if authorized by law to provide such notice; and

(i) to employers for certain medical surveillance work. Any such Disclosures shall be made only after consultation with the HIPAA Compliance Officer.

2. The HIPAA Compliance Officer must be notified upon the receipt of a request from the State Department of Health for information to ensure appropriate reporting.

3. The release of information must be limited to that information that is specified in the request.
   a. Statistical Reports. The State Department of Health is charged with tracking Health Information within the State of Oklahoma. The Department may request Personnel to provide to the Division of Health Care Information (“DHCI”) certain Health Care information for the purpose of statistical and other similar reports. PPMOK may Disclose the requested information without the patient’s written Authorization. This includes discharge data including, but not limited to, complete discharge data sets or comparable information for each patient discharged.

   **Birth Certificates.** If a birth occurs in PPMOK, a birth certificate must be prepared and filed by one of the following Personnel in the indicated order of priority:

   1. The physician in attendance at or immediately after the birth; or

   2. Any other person in attendance at or immediately after the birth.

   3. Personnel must
      a. obtain the personal data,
      b. prepare the certificate,
      c. secure the signatures required by the certificate,
      d. and file the certificate with the local registrar.
      e. The physician in attendance must certify to the facts of birth and provide the medical information required by the certificate within five (5) days after the birth.
      f. No patient Authorization is necessary to disclose the information used to prepare and file the birth certificate.

   **Death Certificates.** A death certificate for each death that occurs in Oklahoma must
1. be filed with the local registrar of the district in which the death occurred,

2. within three (3) days after the death and prior to burial or removal of the body.

3. A funeral director or similar person is responsible for filing the death certificate.

4. the funeral director must complete the certificate of death as to personal data and deliver the certificate, within twenty-four (24) hours after the death, to the attending physician at PPMOK who was responsible for the patient’s care or to the medical examiner.

5. Personnel responsible for the patient’s care or the medical examiner must then complete and sign the certificate of death within forty-eight (48) hours after death.

6. If Personnel in charge of the patient’s care is not in attendance at the time of the death, the medical certificate must be completed and signed within forty-eight (48) hours after death by other Personnel in attendance at the time of death. In this instance, the alternate physician must note on the face of the certificate the name of the attending physician and that the information shown is only as reported.

7. The Authorization of the patient’s Personal Representative is not required to disclose information necessary to complete the certificate of death for filing.

**Communicable or Venereal/Sexually Transmitted Diseases.**

1. **Definitions:**
   a. “communicable disease” means an illness due to a specific infectious agent or its toxic products, arising through transmission of that agent or its products from reservoir to susceptible host, either directly as from an infected person or animal, or indirectly through the agent of an intermediate plant or animal host, a vector, or the inanimate environment. It also means an infestation by an ectoparasite and similar species.
   b. “venereal disease” or “sexually transmitted disease” means syphilis, gonorrhea, chancroid, granuloma inguinale, lymphogranuloma venereum, and any other disease that may be transmitted from any person to any other person through or by means of sexual intercourse and found and declared by medical science or accredited schools of medicine to be infectious or contagious, and declared to be communicable and dangerous to the public health.

2. **Procedure:** PHI relating to communicable or venereal/sexually transmitted disease may be released without patient Authorization under the following limited circumstances, and following consultation with the HIPAA Compliance Officer:
a. **Court Order.** Release of PHI may be made upon receipt of a court order.\(^\text{18}\)

b. **Administrative Orders.** Release of limited PHI relating to venereal/sexually transmitted or communicable diseases may be made to the State Department of Health upon the issuance of a final agency order (an administrative order) issued by an administrative law judge, which is the final order of the State Department of Health, after the administrative law judge determines release is necessary to protect the health and well-being of the general public. In this instance, only the patient’s initials shall be Disclosed unless the order specifies the release of the name of the patient.

c. **Reports of Venereal/Sexually Transmitted Disease.** All Personnel who make a diagnosis or treat a patient for any venereal/sexually transmitted disease, as defined above, must promptly report the case, in writing, to the State Commissioner of Health.

   i. If Personnel know or have good reason to suspect that the patient with a venereal/sexually transmitted disease is conducting him/herself as to expose other persons to infection, or is about to so conduct him or herself in such a way, Personnel must notify the State Commissioner of Health of the name and address of the diseased patient and the essential facts of the case. This information may contain the patient’s PHI.

**Personnel Exposures.** Release is made of medical or epidemiological information to Personnel who have had risk exposure.\(^\text{19}\)

1. **Statistical Disclosures.** Release is made of specific medical or epidemiological information for statistical purposes in such a way that no person can be identified. See De-Identified Information. Policy.

2. **Diagnosis and Treatment.** Release is made of PHI among Personnel within the continuum of care for the purpose of diagnosis and Treatment of a communicable or venereal/sexually transmitted disease of the patient whose information is released.

**Tumor Registry.** The State Commissioner of Health may establish a tumor registry to ensure an accurate and continuing source of data concerning cancerous, precancerous, and tumorous diseases. The tumor registry may include data necessary for epidemiological surveys and scientific research and other data that is necessary to further the recognition, prevention, control, treatment, and cure of cancer and precancerous and tumorous diseases.

---

\(^{18}\) See Section 5 of Judicial and Administrative Procedures for procedure

\(^{19}\) Risk exposure is exposure that is epidemiologically demonstrated to have the potential for transmitting a communicable disease.
1. The Commissioner may require PPMOK, to report the following information regarding cancerous and precancerous and tumorous diseases:
   a. The patient’s name, address, age, race, sex, Social Security Number, and hospital identifier or other identifier;
   b. The patient’s residential, family, environmental, occupational, and medical histories; and
   c. The physician’s name, diagnosis, stage of the disease, and method of treatment and the name and address of any facility providing treatment.

**Health Oversight Activities.** Personnel may disclose PHI to a Health Oversight Agency for certain oversight activities authorized by law, upon receipt of a written request for such. The request must state the purpose for which the PHI is sought. The HIPAA Compliance Officer must be consulted prior to any release of PHI under this section.

**Medicaid Program.** To the extent PPMOK accepts Medicaid, Personnel must provide the Attorney General of the State of Oklahoma access to all records of Medicaid recipients under the Oklahoma Medicaid Program that are

1. held by PPMOK Personnel
2. for the purpose of investigating the crime of Medicaid
3. fraud or for use or potential use in any legal, administrative, or judicial proceeding, upon receipt of a written request for such.
4. The request must indicate the purpose for which the records are sought.
5. The HIPAA Compliance Officer should be consulted prior to release.

**Personnel may not refuse to provide the Oklahoma Health Care Authority or the Oklahoma Attorney General with access to such records on the basis that release would violate the patient’s right of privacy, privilege against Disclosure or Use, or any professional or other privilege or right. The Disclosure of PHI pursuant to this Section will not subject any physician or other health services provider to liability for breach of any confidential relationship between a patient and a provider.**

**Reports of Certain Deaths.** Certain deaths of patients occurring on PPMOK property must be reported by Personnel to the HIPAA Compliance Officer and to Law Enforcement.

1. The HIPAA Compliance Officer must promptly report the death to the Office of the Chief Medical Examiner prior to release of the body.
2. Types of deaths subject to investigation that should be reported include
a. violent deaths;
b. suspicious deaths;
c. deaths related to disease that might constitute a threat to public health;
d. deaths unattended by a physician for a fatal or potentially fatal illness;
e. a death after an unexplained coma;
f. deaths that are medically unexpected and that occur in the course of a therapeutic procedure;
g. a death of an inmate;
h. and deaths of persons who will be cremated, buried at sea, transported out of state, or otherwise made unavailable for pathological study.
i. Within thirty-six (36) hours of death, a written report must be submitted to the Office of the Chief Medical Examiner, which must be accompanied by true and correct copies of all medical records of PPMOK concerning the deceased patient.

3. The Chief Medical Examiner may require PPMOK to produce the patient’s PHI including records, documents, or other items regarding the deceased patient that are necessary to investigate the death. The requested PHI may be Disclosed without the Authorization of the patient’s Personal Representative.
   a. However, PPMOK shall limit disclosure of such PHI to that which is specifically requested by the Chief Medical Examiner.

**Disclosures to Coroners and Medical Examiners.** PPMOK may Disclose PHI to coroners and medical examiners as necessary for the purpose of their identifying a deceased person, determining a cause of death, or carrying out their duties as authorized by law.

1. To the extent necessary, such PHI may be Disclosed prior to, and in reasonable anticipation of, the patient’s death.

2. A written request from the coroner or medical examiner that includes the basis of the request must be obtained prior to the release.

**Disclosure to Funeral Directors.** PPMOK may Disclose PHI to funeral directors as necessary for them to carry out their duties with respect to the decedent. To the extent necessary, such PHI may be Disclosed prior to, and in reasonable anticipation of, the patient’s death. A written request from the funeral director that includes the basis of the request must be obtained prior to the release.

**Cadaveric Organ, Eye or Tissue Donations.** PPMOK may Disclose, without Authorization, PHI to organ procurement organizations or other entities engaged in the procurement, banking, or transplantation of cadaveric organs, eyes, or tissue for the purpose of facilitating organ, eye, or tissue donation and transplantation. A written request from the organ procurement organization that includes the basis of the request must be received prior to the release.
Workers’ Compensation. Under the Oklahoma’s Workers’ Compensation laws, an employer must

1. provide an injured employee with medical, surgical, or other attendance or Treatment; nurse and hospital service; medicine; crutches; and any apparatus as may be necessary after an injury that occurred during the course of employment.

2. The attending physician is required to supply the injured employee and the employer, within seven (7) days after the examination, with a full examining report of injuries found at the time of examination and proposed Treatment. At the conclusion of the Treatment, the attending physician must supply a full report of the Treatment of the injured employee to the employer.

3. The attending physician who renders Treatment to the employee must promptly notify the employee and employer or employer’s insurer in writing after the employee has reached maximum medical improvement and is released from active medical care. If the employee is capable of returning to modified light duty work, the attending physician must promptly notify the employee and the employer or the employer’s insurer in writing and specify what restrictions, if any, must be followed by the employer in order to return the employee to work.

4. The Oklahoma Workers’ Compensation Act contemplates that an employee who participates in the benefits of this Act is deemed to consent to the treating physician is making these reports. Thus, patient Authorization is not required. However, Uses and Disclosures made under this section must be limited only to that PHI which is relevant to the injury for which benefits are sought.

IV. REFERENCES:

1. 45 C.F.R. §164.512 (l); 45 C.F.R. 164.513(2).
2. 10 O.S. § 7102
3. 43A O.S. 10-108.
5. 63 Okla. Stat. 1-317
I. PURPOSE: To articulate conditions under which family and friends may be notified of a patient’s condition.

II. POLICY:

1. Personnel may Disclose PHI to any person identified by a patient, (such as a patient’s family member, other relative, close personal friend), as long as the information Disclosed is relevant to that person’s involvement with the patient’s care or Payment.

2. Personnel may Use or Disclose PHI to notify, or assist in the notification of (including identifying or locating), a family member, a personal representative of the patient, or another person responsible for the care of the patient of the patient’s location, general condition, or death.

3. Personnel may Use or Disclose PHI to a public or private entity authorized by law or by its charter to assist in disaster relief efforts. The PHI that is released shall be limited to the patient’s location, general condition, or death.

III. PROCEDURE:

1. Patient is Present: If the patient is present for, or otherwise available prior to, a Use or Disclosure to a family member or other as described in paragraph II above, and has the capacity to make Health Care decisions, Personnel may Use or Disclose the PHI if Personnel:
   a. Obtain the patient’s agreement;
   b. Provide the patient with the opportunity to object to the disclosure (and the patient does not express an objection) and documents the lack of objection in the patient’s medical record; or
c. Reasonably infer from the circumstances, based on the exercise of professional judgment, that the patient does not object to the Disclosure and notes such in the patient’s medical records.

2. **Patient is Not Present**: If the patient is not present, or cannot consent to the Use or Disclosure of PHI due to incapacity or an emergency circumstance, Personnel may, in the exercise of professional judgment, determine whether the Disclosure in paragraph II above is in the best interests of the patient and, if so, Disclose only the PHI that is directly relevant to the person’s involvement with the patient’s Health Care.

3. **Personnel may elect to use the Authorization for Verbal Release of PHI (available on the HIPAA website) as a mechanism for documenting the patient’s agreement to verbal Disclosures.**

4. Personnel may use professional judgment and experience with common practice to make reasonable inferences of the patient’s best interest in allowing a person to act on behalf of the patient to pick up filled prescriptions, medical supplies, X-rays, or other PHI.

5. The following criteria should be considered when determining whether it is in the patient’s best interest to Disclose the PHI to another person:
   a. Whether the potential Disclosure is common practice;
   b. The nature of the relationship between the parties;
   c. The sensitive nature of the information being Disclosed;
   d. The ability of the patient to manage necessary tasks (e.g., pick up prescriptions, medical supplies, x-rays, or other forms of PHI); and
   e. Whether an incapacitated patient is a suspected victim of domestic violence and whether the person seeking information may have abused the patient. In these instances, Personnel should not Disclose information to the suspected abuser if there is reason to believe that such a Disclosure could cause the patient harm.
   f. Personnel are not required to verify the relationship of relatives or other individuals involved in the patient’s care, unless they have reason to doubt the relationship.
      i. Personnel should inquire into the individual’s relationship with the patient and document it. The patient’s act of involving the other person in his/her care also may suffice as verification of identity.

6. Personnel should contact the Compliance Officer with questions regarding this policy.

IV. REFERENCES:

1. AMC HIPAA Privacy Guidelines, PRIV. 23 (pg. 119).
2. HIPAA Privacy Regulations, 45 C.F.R. 164.510(b).
I. PURPOSE: To set forth requirements regarding Uses and Disclosures of PHI to Business Associates.

II. POLICY: PPMOK may Disclose PHI to a Business Associate, and may allow a Business Associate to create or receive PHI on its behalf, if PPMOK ensures that it has executed an agreement with the Business Associate that contains language requiring the Business Associate to appropriately safeguard the PHI (a “Business Associate Agreement”), in compliance with HIPAA and HITECH.

1. If PPMOK knows of a pattern of activity or practice of a Business Associate that constitutes a material breach or violation of the Business Associate’s obligation under the Business Associate Agreement, PPMOK must take reasonable steps to cure the breach or end the violation.

2. If such steps are unsuccessful, or cure is not possible, the Business Associate Agreement must be terminated.

3. If termination is not possible, the problem with the Business Associate must be reported to the Secretary of the Department of Health and Human Services by the HIPAA Compliance Officer.

III. PROCEDURE:

1. PPMOK must identify its Business Associates and bring the need for contractual language to the attention of the HIPAA Compliance Officer when PPMOK routes a contract for signature.

---

20 Business Associate is a person or entity who provides certain functions, activities, or services on behalf of PPMOK that involve the Use and/or Disclosure of PHI.
2. The HIPAA Compliance Officer is responsible for drafting, implementing, and updating the appropriate Business Associate language and/or agreements to comply with the requirements of HIPAA and HITECH. All contracts must be reviewed by legal counsel and the HIPAA Compliance Officer.
   a. Business Associate language must be included in applicable new and renewing contracts.

3. Questions regarding the status of a vendor or independent contractor as a Business Associate should be forwarded to the HIPAA Compliance Officer.

4. Questions regarding whether a vendor has a Business Associate Agreement in place with PPMOK should be directed to the HIPAA Compliance Officer.

5. Questions regarding whether any other entities have a Business Associate Agreement in place with PPMOK should be directed to HIPAA Compliance Officer.

IV. REFERENCES:

1. AMC HIPAA Privacy Guidelines, PRIV. 03 and .16 (pg. 70 and 108).
2. HIPAA Privacy Regulations, 45 C.F.R. Part 164, Subpart D.
I. PURPOSE: To set forth requirements regarding the Use and Disclosure of PHI for Marketing.

II. POLICY:

1. PPMOK must obtain an Authorization for any Use or Disclosure of PHI for Marketing, unless the communication is in the form of:
   a. a face-to-face communication made by Personnel to an individual; or
   b. a promotional gift of nominal value provided by PPMOK.

2. “Marketing” is defined as a communication about a product or service that encourages the purchase or use of the product or service, except for communications made:
   a. to describe a health-related product or service that is provided by PPMOK;
      i. for the Treatment of the individual;
      ii. for case management or care coordination of the individual, or
      iii. to direct or recommend alternative treatments, therapies, providers, or settings of care to the individual. (These communications are more likely Health Care Operations.)

3. If PPMOK has received payment in exchange for making one of those communications, the communication may not be considered Health Care Operations unless:
   a. the communication describes only a drug or biologic that is currently being prescribed for the recipient of the communication and any payment is reasonable in amount;
   b. the communication is made by PPMOK and individual Authorization is obtained; or
   c. the communication is made by a Business Associate on behalf of PPMOK and the communication is made consistent with the Business Associate agreement.
d. If the Marketing involves direct or indirect payment to PPMOK from a third party, the Authorization must state that payment is involved. The HIPAA Compliance Officer must be contacted to develop or review the proposed Authorization to ensure it complies with this Policy.

4. Personnel are prohibited from selling patient lists to third parties and from disclosing PHI to a third party for the independent Marketing activities of the third party, without obtaining an Authorization from every patient on the list.

5. PPMOK may not directly or indirectly receive remuneration in exchange for PHI unless Authorized by the individual. However, that general rule does not apply if the purpose or the remuneration is for:

Public Health activities:

- Research purposes where the price charged reflects the cost of preparation and transmittal of the information;
- Treatment of the individual;
- Health Care Operations related to the sale, merger, or consolidation of a covered entity;
- Performance of services by a Business Associate on behalf of PPMOK;
- Providing the individual with a copy of the PHI maintained about him/her; or
- Other reasons determined necessary and appropriate by the Secretary of the Department of Health and Human Services.

III. PROCEDURE: If PPMOK wishes to use or Disclose PHI for Marketing purposes must contact the HIPAA Compliance Officer, who will assist in providing a HIPAA compliant Authorization.

1. Authorizations for Marketing must be kept in a patient’s medical record for at least six (6) years from the date of signature.

IV. REFERENCES:

1. AMC HIPAA Privacy Guidelines, PRIV. 24 (pg. 121).
2. HIPAA Privacy Regulations, 45 C.F.R. 164.508(a)(3).
I. PURPOSE To establish permitted Uses and Disclosure of PHI in Research.

II. POLICY: At this time, PPMOK does not participate in any Research activities. However, if at any point in the future, PPMOK begins to participate in Research, it shall establish policies and procedures similar to the following:

PPMOK may Use and Disclose PHI for the purposes of Research only in accordance with its policies. PPMOK shall work with the HIPAA Compliance Officer regarding privacy issues arising in connection with the research.

1. The Use or Disclosure of PHI in Research requires one of the following, in accordance with PPMOK policies:
   a. Authorization for the Use of Disclosure of PHI;
   b. Waiver of the Authorization requirement by the Privacy Committee;
   c. De-identification of the PHI; or
   d. Use of a Limited Data Set, with accompanying Data Use Agreement\(^{21}\)

2. Authorizations must comply with PPMOK Privacy and Security policies.

III. PROCEDURE: All Research that will involve the Use or Disclosure of PHI must be submitted to the HIPAA Compliance Officer and must be accompanied by the appropriate IRC Privacy forms. Revisions to these forms must be approved by the Privacy Committee and the HIPAA Compliance Officer.

1. The HIPAA Compliance Officer and the Research Committee will jointly determine whether the proposed Use or Disclosure of PHI complies with the applicable provisions of HIPAA.

2. Research involving the Use or Disclosure of De-Identified Health Information or Limited Data Sets must comply with RC policies as well as the privacy policies regarding, Limited Data Sets and De-Identified information.

\(^{21}\) (available on the HIPAA forms webpage and from the HIPAA Compliance Officer.)
3. Persons conducting Research involving PHI are responsible for logging Disclosures, pursuant to the Accounting of Disclosures policy.

IV. REFERENCES

1. HIPAA Privacy Regulations, 45 CFR § 164.512(i).
I. PURPOSE: To establish permitted Uses and Disclosures of limited data sets -- PHI from which certain identifiers have been removed -- and the method for creating them.

II. POLICY: PPMOK may Use and Disclose a limited data set without patient Authorization only for the purposes of Research, public health, or Health Care Operations and if PPMOK enters into a Data Use Agreement with the intended recipient of the limited data set.

1. A limited data set is PHI that does not directly identify the patient, but contains certain potentially identifying information.

2. PPMOK may use PHI to create a limited data set or Disclose PHI to a Business Associate to create a limited data set on behalf of PPMOK.

3. If PPMOK learns of or knows of a pattern of activity or practice of the limited data set recipient that constitutes a material breach or violation of the Data Use Agreement, it must take reasonable steps to cure the breach or end the violation, as applicable. If such steps are unsuccessful or the breach cannot be cured, PPMOK must discontinue Disclosure of PHI to the recipient and report the problem to the HIPAA Compliance Officer, for report to Secretary of the Department of Health and Human Services.

III. PROCEDURE:

1. Limited Data Set. In order to create a limited data set, the following direct identifiers of the patient or of relatives, employers, or household members of the patient must be removed:
   a. Names
   b. Postal address information, other than town, city, state, and zip code
   c. Telephone numbers
   d. Fax numbers
   e. Electronic mail addresses
f. Social Security Numbers

h. Health plan beneficiary numbers

i. Account numbers

j. Certificate/license numbers

k. Vehicle identifiers and serial numbers, including license plate numbers

l. Device identifiers and serial numbers Web Universal Resource Locators (URLs)

m. Internet Protocol (IP) address numbers

n. Biometric identifiers, including fingerprints and voiceprints

o. Full-face photographs and comparable images

p. The patient’s birth date should be Disclosed only if PPMOK and the recipient of the information agree that it is needed for their purpose.

2. Data Use Agreements. All Data Use Agreements must be approved by the HIPAA Compliance Officer or legal counsel prior to execution. A sample Data Use Agreement is available on the HIPAA forms webpage and from the HIPAA Compliance Officer. A Data Use Agreement must:

   a. Establish the permitted Uses and Disclosures of the limited data set.
   b. Establish who is permitted to Use or receive the limited data set.
   c. Provide that the recipient of the information will:
      d. Not use or further Disclose the information other than as permitted by the Data Use Agreement
      e. Use appropriate safeguards to prevent Use or Disclosure of the information other than as permitted by the agreement
      f. Report to PPMOK any Uses or Disclosures the recipient is aware of that are not provided for by the Data Use Agreement
      g. Ensure that the recipient’s agents who have access to the information agree to the same restrictions as imposed on the recipient
      h. Not use the information to identify the individuals or contact the individuals

IV. REFERENCES:

1. HIPAA Privacy Regulations, 45CFR § 64.514 (e).
2. Sample Data Use Agreement – available on the HIPAA forms webpage and from the HIPAA Compliance Officer.
I. PURPOSE: To establish the method and policy for de-identifying and re-identifying PHI.

II. POLICY:

De-Identified Information/Re-Identification: PPMOK may Use and Disclose de-identified health information without regard to the Privacy Policies or Regulations as long as the code or other means of identification designed to permit re-identification is not disclosed.

1. PPMOK may Use PHI to create information that is not Individually Identifiable Health Information or Disclose PHI to a Business Associate to de-identify Health Information on behalf of PPMOK. If de-identified information is re-identified, its Use and Disclosure become subject to regulation under the Privacy Policies and Regulations.

2. Health Information that does not identify an individual and for which there is no reasonable basis to believe that the Health Information can be used to identify the patient is “de-identified information” and is not individually identifiable or considered Protected Health Information. It is not subject to the requirements of this Policy or the Privacy Regulations.

III. PROCEDURE:

1. De-identification: Health Information can be de-identified by using one of the two methods listed below:
   a. Safe Harbor. The following identifiers of the patient or of the relatives, employers, or household members of the patient are removed and PPMOK has no actual knowledge that the information could be used alone or with other information to identify the individual:
      i. Names
ii. All geographic subdivisions smaller than a state, including street address, city, county, and zip code and equivalent geocodes, except for the initial 3 digits of a zip code if, according to current publicly available data from the Census Bureau:

   1. the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people, and

iii. the initial 3 digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000 (example, for the zip code 73069, all areas using the zip code beginning with 730 have more than 20,000 in the aggregate).

iv. All elements of dates (except year) for dates directly related to the patient, including birth date, admission date, discharge date, date of death; all ages over 89; and all elements of dates (including year) indicative of such age. (Exception: Ages and elements may be aggregated into a single category of age 90 or older.)

v. Telephone numbers

vi. Fax Numbers

vii. E-mail addresses

viii. Social Security Numbers

ix. Medical record numbers

x. Health plan beneficiary numbers

xi. Account numbers

xii. Certificate/license numbers

xiii. Vehicle identifiers, serial numbers, license plate numbers

xiv. Device identifiers and serial numbers

xv. Web Universal Resource Locators (URLs)

xvi. Internet Protocol (IP) address numbers

xvii. Biometric identifiers, including fingerprints and voiceprints

xviii. Full face photographic images and other comparable images

xix. All other unique identifying numbers, characteristics, or codes.

b. Alternative Method of De-Identification. A biostatistician or other person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable must apply such principles and methods and determine that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify the individual who is the subject of the information. The person making this determination must be an independent third party and must document the methods and results of the analysis that justify the determination.
2. **Re-Identification:** PPMOK may assign a code or other means of record identification to allow de-identified information to be re-identified, provided that:
   a. **Derivation.** The code or other means of record identification is not derived from or related to information about the individual and is not otherwise capable of being translated so as to identify the individual; and
   b. **Security.** The code and/or mechanism for re-identification is not Used or Disclosed for any other purpose.

**IV. REFERENCES:**

1. AMC HIPAA Privacy Guidelines, PRIV-15 (pg. 107).
2. HIPAA Privacy Regulations, 45 C.F.R. 164.502(a); 45 C.F.R. 164.514 (a) – (c)
I. PURPOSE: To establish requirements for including a patient’s name in a Facility Directory. PPMOK does not currently have ANY in-patient facilities. As such, there is no current need for a Facility Directory. In the event a need for a Facility Directory is identified, a Facility directory shall be formally approved and created.

II. POLICY: PPMOK does not currently have, or have any need for a facility directory. However, should PPMOK establish a facility at a future date, PPMOK would establish privacy policies similar to the following:

PPMOK may Use or Disclose certain PHI without the written Authorization of the patient for the purpose of maintaining a Facility Directory. The following PHI may be Used in a Facility Directory:

1. The patient’s name.

2. The patient’s location within the Facility. PPMOK may not release information that indicates a patient is being treated in an area that is limited to Treatment of certain diseases or conditions, such as alcohol or drug rehabilitation, detoxification, psychiatric treatment, or communicable disease treatment.

3. The patient’s condition described in general terms (such as stable, fair, serious) that does not communicate specific medical information.

4. The patient’s religious affiliation (may be Disclosed to members of the clergy only). The information in a Facility Directory may be Disclosed to any person who asks for the patient by name.
   a. However, a patient’s religious affiliation may be Disclosed only to members of the clergy.
III. PROCEDURE:

1. At the time of registration, patients must be informed, either orally or in writing, of PPMOK’s intent to Use or Disclose certain PHI in the Facility Directory. The patient must be informed of the type of information that will be Disclosed and the persons to whom the information may be disclosed.

2. If the patient indicates that he/she does not want to be included in the Facility Directory, he/she should be asked to complete the “Directory Opt-Out” form.

3. In an emergency situation, PPMOK may include the patient’s information in a Facility Directory if its Personnel determine it is in the patient’s best interest. PPMOK must give the patient the opportunity to object to the placement in the directory as soon as it becomes practicable to do so.

IV. REFERENCES:

1. AMC HIPAA Privacy Guidelines, PRIV. 22 (pg. 117).
2. HIPAA Privacy Regulations, 45 C.F.R. 164.510(a).

---

22 At the time a facility directory is used, then all appropriate forms will be placed on the website.
I. PURPOSE: To provide for notification in the case of breaches of unsecured PHI. For purposes of these requirements, section 13402(h) of the HITECH Act defines “unsecured PHI” as PHI which is not secured through the use of approved technologies or methodologies.

- To be approved, technologies and methodologies must render PHI unusable, unreadable, or indecipherable to unauthorized individuals.

II. POLICY: PPMOK will implement reasonable and appropriate technologies and methodologies designed to secure PHI from unauthorized Disclosure. (If PHI is rendered unusable, unreadable, or indecipherable to unauthorized individuals, then the PHI is not “unsecured” PHI.)

1. This Policy establishes the requirements outlined by HITECH regarding the protection of PHI that PPMOK must comply with and the notification that must occur in the event of a breach. The breach notification provisions of HITECH apply to HIPAA Covered Entities and their Business Associates that access, maintain, retain, modify, record, store, destroy, or otherwise hold, Use, or Disclose unsecured PHI.
   a. PHI secured by one of the above methods is not unsecure and is therefore not subject to this policy.

2. The PPMOK supervisor shall be responsible for compliance with this Policy, in coordination with the HIPAA Compliance Officer.

3. Methods of Protection: Either of the following methods may be used to secure PHI and make it unusable, unreadable, or indecipherable to unauthorized individuals.
   a. Encryption: All PHI shall be encrypted during storage and transmission at a level which meets or exceeds current industry standards as set forth by NIST, and which complies with HIPAA and HITECH regulations.
b. **Destruction**\(^2\): PPMOK will comply with the destruction techniques implemented by IT Security and the HIPAA Compliance Officer that render PHI unusable and/or unreadable in any format.
   
i. Refer to Safeguards policy, for destruction requirements of paper records containing PHI.
   
   ii. PPMOK is not currently destroying any electronic health records, and as such does not have a destruction policy in place.
   
   iii. All hardware, devices and machines containing ePHI shall be scrubbed of data in accordance with current NIST standards, and in compliance with HIPAA and HITECH regulations.

   1. If a device or piece of hardware is unable to be scrubbed of data, but is physically present, then the device shall be physically destroyed to a point at which it is impossible to physically restore said device to working order. (Devices may be crushed or burned.)

   iv. Devices which have been lost or stolen should be remotely wiped of all data if at all possible.

   4. For additional information on the guidelines and standards of encryption and destruction methods of electronic PHI, contact the HIPAA Compliance Officer.

**Notification of Breach:** If a breach of PHI or ePHI is discovered, the HIPAA Compliance Officer must be notified immediately. The Officer will determine, using the HITECH/HIPAA Breach Notification Reporting Process, whether and when a notice to the individual, the media, and/or HHS is appropriate and, if so, the content of the notice.

1. In the event a breach of unsecured PHI, the HIPAA Compliance Officer may be required to notify each individual whose unsecured PHI has been, or is reasonably believed to have been, inappropriately accessed, acquired, or disclosed. The HIPAA Compliance Officer shall make such notice according to the requirements of HITECH:

2. Written notice to the individual (or next of kin or personal representative if the individual is deceased) at the last known address of the individual (or next of kin) by first-class mail (or by electronic mail if agreed to by the individual);

3. In the case in which there is insufficient or out-of-date contact information (excluding for next-of-kin or personal representative), substitute notice shall be provided. In cases of fewer than 10 individuals for whom there is insufficient or out-of-date contact information, substitute notice may be by an alternative form of written notice, telephone, or other means.

\(^2\) Refer to PPMOK Security policies) for destruction requirements of electronic PHI
4. In the case of 10 or more individuals for whom there is insufficient contact information, conspicuous posting for 90 days consecutive days on the home page of PPMOK’s web site and/or notice in major print or broadcast media, each including a toll-free number, will occur, as determined by the HIPAA Compliance Officer.

5. In cases that PPMOK or the HIPAA Compliance Officer deem urgent based on the possibility of imminent misuse of the unsecured PHI, notice by telephone or other method is permitted in addition to the above methods.
   a. Details of the notice shall include the following: (A sample letter is available from the HIPAA Compliance Officer.)
      i. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;
      ii. A description of the types of unsecured PHI that were involved in the breach (such as full name, SSN, DOB, home address, account number, or disability code);
      iii. The steps individuals should take to protect themselves from potential harm resulting from the breach;
      iv. A brief description of what PPMOK is doing to investigate the breach, mitigate losses, and protect against any further breaches;
      v. Contact procedures for individuals to ask questions or learn additional information, which shall generally include a toll-free telephone number, an e-mail address, web site, or postal address.

6. If a breach is caused or discovered by a Business Associate of PPMOK, the HIPAA Compliance Officer shall work with the Business Associate to address the notice requirements, in accordance with the terms of the Business Associate Agreement in place between the parties. The timing and content of any required notice shall be in accordance with applicable law.

7. If a Law Enforcement Official informs PPMOK or its Business Associate that a required notice would impede a criminal investigation or threaten national security, the HIPAA Compliance Officer shall
   a. comply with Law Enforcement’s written request for a delay for the time period specified in the statement or
   b. document Law Enforcement’s verbal request, specifying the time for which the delay is required and the identity of the Law Enforcement Official making the request and delay the notice for up to 30 days, unless a written statement with a longer delay period is provided.
Tracking: PPMOK must maintain a log of breaches of unsecure PHI and shall promptly notify the HIPAA Compliance Officer of each breach.

1. PPMOK, shall maintain a log of all reported breaches of unsecure PHI and shall submit required reports of such to the Secretary of HHS annually, as required by the Act.

IV. REFERENCES:

1. HIPAA Privacy Rules 45 CFR Parts 400, et seq.
2. NIST SP 800-111 “Guide to Storage Encryption Technologies for End User Devices” and SP 800-88 “Guidelines for Media Sanitization” as updated or revised
3. 24 O.S. 163.5 Breach Notification Reporting Process (available from the University Official)
Privacy Audit Program

I. PURPOSE: To set forth PPMOK’s HIPAA Privacy Audit Program.

II. POLICY: The HIPAA Compliance Officer will maintain a HIPAA Privacy Audit Program, and shall maintain all documentation pertaining to said Audit Program.

III. PROCEDURE: The HIPAA Compliance Officer shall conduct HIPAA compliance audits. Audit instruments shall be updated as needed by the HIPAA Compliance Officer to address current and ongoing HIPAA issues.

1. The HIPAA Privacy Audit Program shall include, at a minimum, the following:
   a. In-person audits of each facility and office, occurring approximately once every 12 months, or more often if indicated by audit results or HIPAA incidents.
   b. In-person audits of off-site storage facilities where PHI is stored by PPMOK, occurring approximately every 12 months, or more often if indicated by audit results or HIPAA incidents.
   c. Coordination between management, facility supervisors and the HIPAA Compliance Officer regarding audit issues, items, and findings.
   d. Regular audits of the Company’s Business Associates, either in person or via written compliance certification.

2. The HIPAA Compliance Officer shall prepare the audit reports within two weeks of conducting the audit.

3. The HIPAA Compliance Officer will provide management, and the facility supervisor with a written response to each in-person audit report, and shall notify PPMOK in writing of the audit results, including any corrective steps required.
4. The HIPAA Compliance Officer shall review the quarterly self-audits and notify PPMOK if the audit indicates the need for corrective action or additional training.

5. The HIPAA Compliance Officer shall notify PPMOK if any Business Associate fails to comply with the Company’s audit, necessitating termination of the Business Associate arrangement and/or reporting to the Secretary of Health and Human Services.

6. The HIPAA Compliance Officer or the Office of Compliance will maintain such documentation for at least six (6 years).

IV. REFERENCES:

1. HIPAA Privacy Regulations, 45 CFR §164.306.
Security Policies
I. POLICY

A. It shall be the policy of PPMOK to protect and safeguard the electronic Protected Health Information (ePHI) created, acquired, and maintained by it as follows:

1. Ensure the Confidentiality, Integrity, and Availability of all ePHI that it creates, receives, maintains, or transmits;

2. Protect against any reasonably anticipated threats or hazards to the security or Integrity of such information;

3. Protect against any reasonably anticipated Uses or Disclosures of such information that are not permitted or required under the HIPAA Privacy or Security rules, and

4. Ensure its Workforce Members comply with these HIPAA Security policies.

B. These policies supersede any conflicting policies and procedures of any PPMOK relating to the protection of ePHI and of Information Systems. PPMOK may maintain additional policies and procedures relating to the protection of ePHI and Information Systems only to the extent that they do not conflict with these policies. PPMOK may add to or supplement these policies, but they may not delete any without first consulting the HIPAA Compliance Officer.

II. REFERENCES

1. 45 CFR 164.304
2. 45 CFR 164.306
I. PURPOSE: To identify the security responsibilities of the HIPAA Compliance Officer.

II. POLICY The HIPAA Compliance Officer’s responsibilities include, but are not limited to:

1. Ensuring that necessary and appropriate Security policies are developed, implemented, and maintained to safeguard the integrity, confidentiality, and availability of ePHI. Reviewing and modifying Security policies as needed to ensure reasonable and appropriate protection of ePHI.

2. Retaining all versions of Security policies and related documentation for at least six years from the date of creation or date of last effect, whichever is longer.

3. Making the Security policies and forms available to all Personnel, and providing training to Personnel. Training materials should include a test or other opportunity to demonstrate understanding of the information presented.


5. Performing annual HIPAA Security risk assessments, developing and reviewing management plans for identified risks and vulnerabilities, and advising PPMOK, generally, of HIPAA Security risks.

6. Investigating, mitigating, and resolving HIPAA incidents involving ePHI.

III. REFERENCES

1. 45 CFR 164.308(a)(2)
2. 45 CFR 164.316
I. DEFINITIONS: Unless otherwise provided, the definitions below apply to all of PPMOK’s Security policies. These terms are capitalized when used in the HIPAA Security policies to indicate that they have been uniquely defined by PPMOK.

Any capitalized terms in HIPAA Security policies that are not defined below are defined in the HIPAA Privacy policy, Definitions.

1. **Access**: The ability or means necessary to read, write, modify, or communicate data/information or otherwise use any system resource. (This definition is NOT applicable to the HIPAA Privacy policies.)

2. **Administrative Safeguards**: Administrative actions, policies, and procedures to manage the selection, development, implementation, and maintenance of measures to protect ePHI and manage the conduct of Workforce Members in relation to protecting ePHI.

3. **Authentication**: Corroboration that a person is who he says he is.

4. **Availability**: Means data or information is accessible and usable upon demand by an authorized person.

5. **Business Impact Analysis (BIA)**: An exercise that determines the impact of losing the support of any resource to PPMOK, establishes the escalation of that loss over time, identifies the minimum resources needed to recover, and prioritizes the recovery of processes and supporting systems.

6. **Confidentiality**: The keeping of data or information from unauthorized Disclosure.

7. **Control**: A safeguard or countermeasure. Any administrative, management, technical, or legal method that is used to manage risk related to the confidentiality, integrity, and
availability of data and IT resources. Controls include practices, policies, procedures, programs, techniques, guidelines, organizational structures, and the like.

8. **Control Review**: A part of the risk management process that compares existing controls for data and/or information resources with respect to defined security requirements.

9. **Encryption**: Use of an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without the use of a confidential process or key.

10. **ePHI**: Electronic Protected Health Information; individually identifiable health information maintained or transmitted in electronic form or media.

11. **Facility**: The physical premises and the interior and exterior of buildings.

12. **Information Security Incident** –
   a. The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an Information System.
   b. A security-related incident that is known to or has the potential to negatively impact the confidentiality, integrity, or availability of information
   c. A violation or imminent threat of violation of Information System policies, standards, or practices
   d. Examples of Information Security Incidents include lost laptops or smart phones, hacking, password cracking, computer virus infection, denial of service attack, or violation or acceptable use of Information Systems.
   e. Information Security Incidents do not include adverse events that are not security-related, such as natural disasters and power failures.

13. **Information Systems**: An interconnected set of information resources under the same direct management control that shares common functionality. Typically includes hardware, software, information, data, applications, communications, and people.

14. **Integrity**: Data which has not been altered or destroyed in an unauthorized manner.

15. **Malicious Software**: Software such as a virus designed to damage or disrupt an Information System.

16. **Password**: A confidential Authentication composed of a string of characters.
17. Physical Safeguards: Physical measures, policies, and procedures designed to protect electronic Information Systems and related buildings and equipment from unauthorized Access and natural and environmental hazards.

18. Resource Owner: The individual or entity that owns the resource and has authority to approve the execution of and/or accept the outcomes resulting from the resource. The Resource Owner may or may not be the owner of the data associated with the resource.

19. Risk: The likelihood that a specific threat will exploit a specific vulnerability, as well as the resulting impact of that event.

20. Risk Analysis/Risk Assessment: The process of identifying, estimating, and prioritizing risks to PPMOK operations, company assets, individuals, and other organizations resulting from the operation of an Information System.

21. Risk Management: The program and supporting processes to manage Information Security risk to PPMOK operations, company assets, individuals, and other organizations, including (a) establishing the context for risk-related activities; (b) assessing risk; (c) responding to risk once it is determined; and (d) monitoring risk over time. PPMOK can manage risk via (a) risk acceptance, (b) risk avoidance, (c) risk mitigation, and (d) risk transference.


23. Technical Product Review: Part of the Risk Management process used to identify risks of technology products and determine appropriate responses and controls.

24. Technical Safeguards: Technology and the related policies and procedures for use of the technology that control Access to and protect ePHI.

25. User: A person or entity authorized to access ePHI.

26. Workstation: An electronic computing device, such as a desktop, laptop, or other device that performs similar functions, as well as the electronic media stored in its immediate environment.

II. REFERENCES

1. 45 CFR 164.304
2. HIPAA Privacy policy, Definitions
Device and Media Controls

I. PURPOSE: To establish requirements regarding tracking devices and media containing ePHI into, out of, and within the PPMOK’s facilities.

II. POLICY: PPMOK must develop and implement device and media control policies and procedures to track the receipt and removal of hardware and electronic devices containing ePHI.

III. PROCEDURE: Device and media control policies must address, at a minimum, the following:

1. Disposal and Reuse Procedures: To ensure that data and software are properly removed from hardware and electronic devices that contain ePHI before their disposal or reuse, PPMOK must:
   a. If a Workforce Member is no longer authorized to use the device or media or is voluntarily or involuntarily terminated, the HIPAA Compliance Officer shall ask the Workforce Member to certify that he/she has not retained any sensitive data or made or kept copies of sensitive data. This should be done as part of the check-out process using the Property Clearance Checklist; and
   b. When an company- or personally-owned device that contains ePHI is no longer needed for business or will be reused for a different purpose, all PPMOK data must be completely removed with erase tools that meet industry standards for data destruction.
   c. PPMOK shall log the disposal of its company devices and electronic media. At a minimum, the log must include the following information:
      i. Date and time of disposal
      ii. Who performed the disposal
      iii. Brief description of media or information systems disposed of
      iv. Reason for disposal
v. Verification of data removal or destruction prior to disposal

2. The HIPAA Compliance Officer shall maintain an inventory of PPMOK’s devices and media that contain ePHI, and devices owned by Personnel or others that contain ePHI.

3. The HIPAA Compliance Officer shall reconcile the inventory annually.

4. The inventory should include a description of the device or media, serial number if available, to whom the device or media is assigned, where it is typically maintained, when it was assigned, and when it is returned.

5. If the device or media will be moved, then if appropriate, a back-up copy of the ePHI should be made first.

6. The HIPAA Compliance Officer shall maintain PPMOK’s device and media inventory, completed Property Clearance Checklists, and Disposal Logs. Copies of all logs shall be maintained for six years.

IV. REFERENCES

1. 45 CFR 310(d)
I. PURPOSE To establish policies and procedures to limit physical Access to electronic Information Systems and protect Facilities where ePHI is stored from unauthorized physical access, tampering, and theft.

II. POLICY: PPMOK must protect its ePHI by controlling and monitoring physical access to its facility. PPMOK shall develop and implement procedures designed to control and monitor Access to ePHI.

III. PROCEDURE: PPMOK shall establish Facility access control procedures that must include, but are not limited to, requirements to maintain the following:

1. A current Role-Based Access Worksheet on each Workforce Member.

2. A log of Personnel who have been given a key, key card, or access code that gives them access to Facilities or areas where ePHI is maintained. This log must be updated when Personnel leave PPMOK or work functions change.

3. A log of non-Personnel, excluding patients, who need regular or recurrent access to areas where ePHI is maintained. Logs should include name of person, date, purpose of access, and any other relevant details.

4. A log of physical access by individuals retrieving back-up media, when feasible. Logs should include name, date, materials removed, and other appropriate details.

The HIPAA Compliance Officer shall periodically review physical security of any site containing ePHI, especially after any significant change that may affect the security of data and applications at a particular site.

1. Required access control procedures must include the following:
   a. Entrances and exits that are not monitored or attended must remain locked at all times. Doors must not be propped open.
b. Workforce Members with access to restricted areas must not allow unauthorized individuals access to those restricted areas and should report to management any unidentified persons who have gained, or seek to gain, access.

c. When practicable and depending on the value and sensitivity of the equipment and PHI in the area, entrances, exits, windows, strategic areas of the building, and other means of Access into the building should be alarmed, monitored, or covered by a security camera.

d. Network Wiring/Communications Closets – These locations house network termination equipment including switches and routers. PPMOK shall keep doors to any closets located in its Facility locked and limit key distribution to prevent unauthorized access.

IV. REFERENCES
1. 45 CFR 164.310(a)(1)
2. 45 CFR 164.310(b)
3. HIPAA Privacy Policy, Safeguards
I. PURPOSE: To ensure PPMOK’s HIPAA Security risk analyses and management plans represent an accurate and thorough assessment of and response to potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by PPMOK, as required by HIPAA.

II. POLICY: PPMOK’s HIPAA Compliance Officer shall conduct an annual risk assessment, to identify potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI. PPMOK shall cooperate with its HIPAA Compliance Officer in performing the risk analysis and implementing risk management activities and programs, in accordance with applicable policies. A sample risk analysis form is attached to this policy.

III. PROCEDURE: The HIPAA Compliance Officer shall perform an annual Risk Analysis to identify potential risks and vulnerabilities to the confidentiality, integrity, and availability of PPMOK’s ePHI.

The risk analysis shall include at a minimum the following:

1. Identifying controls that are in place for each Information System, such as physical security, passwords, and audit capability.

2. Identifying risks to the Information Systems and ePHI, under the current controls, such as unauthorized access or loss/theft.

3. Identifying controls that are needed to address the risks, such as additional locks or system upgrades, and whether/how those controls can be implemented.

Risk Management: Based on the results of the risk analysis, PPMOK, in coordination with the HIPAA Compliance Officer, shall develop a management plan to reduce the risks and vulnerabilities identified to a reasonable level, designed to:

1. Ensure the confidentiality, integrity, and availability of its ePHI;
2. Protect against reasonably anticipated threats or hazards to its ePHI;
3. Protect against reasonable anticipated unauthorized Uses or Disclosures of its ePHI; and
4. Ensure compliance with HIPAA by its Personnel.
**Reporting and Resolution:** The HIPAA Compliance Officer shall provide PPMOK with a copy of the risk analysis and risk management plan. If the Officer identifies additional risks or vulnerabilities or areas that need to be managed further, PPMOK shall cooperate with him or her to address each.

**IV. REFERENCES**

1. 45 CFR 164.308(a)(1)(ii)(A)&(B)
2. 45 CFR 164.306(a)(1)-(4)

**SAMPLE RISK ANALYSIS FORM**

PPMOK  
6717 S. Yale Ave., Suite 210  
Tulsa, OK 74136  
____________________(month), 2014  

Item Existing Risk to Risk Additional Control/Control ePHI Posed By: Management Needed  
1.  
2.  
3.  
4.  
5.  
6.  
7.  
8.  

Performed by: ________________________________  
Print Name: ________________________________
I. PURPOSE: To describe the Technical Safeguards that must be in place to protect PPMOK’s ePHI from unauthorized alteration or destruction.

II. POLICY: PPMOK shall have Technical Safeguards in place to protect the ePHI it maintains on its Information Systems from unauthorized alteration or destruction.

III. PROCEDURE: As part of its Technical Safeguards, PPMOK shall comply with or provide for the following:

1. **Integrity of ePHI**: protect ePHI from improper alteration or destruction during storage and transmission
   a. All access to ePHI must require Authentication of Users to the Information System.

2. **Authentication of ePHI**: corroborate that ePHI has not been altered or destroyed in an unauthorized manner.
   a. PPMOK shall establish Technical Safeguards to authenticate ePHI.

3. **User Authentication**: verify the identity of the person or entity seeking Access to ePHI.
   a. PPMOK shall establish a password management policy and provide training to its Workforce Members for properly managing their passwords. At a minimum, its password management policy must:
      i. Require the use of individual passwords to maintain accountability.
      ii. Allow Workforce Members to select and change their passwords.
      iii. Require unique passwords that meet the standards defined by IT.
      iv. Require regular password changes
      v. Not display passwords in clear text when they are being input
      vi. Require storage of passwords in an encrypted form
      vii. Require secure delivery of passwords to Users
viii. Require that default vendor passwords be reset upon installation of software or hardware
ix. Require randomly generated temporary passwords, and force password change at first log-on,
b. PPMOK’s password management training and awareness program must include requirements for use of Information Systems, including:
i. The importance of keeping passwords confidential
ii. The need to avoid maintaining a paper record of passwords, unless the record is stored securely
iii. The need to change passwords when compromise of the system or password may have occurred
iv. IT’s password standards
v. The importance of not using the same password for personal and business accounts
vi. The importance of changing passwords regularly and of not reusing passwords
vii. The need to change temporary passwords at first log-on
viii. The importance of not including passwords in automated log-on processes (e.g., storing in a browser or function key)
ix. The need for Workforce Members to understand that activities involving their user identification and password will be attributed to them

4. Encryption and Decryption of ePHI
   a. ePHI must be encrypted when stored on Information Systems
   b. ePHI sent via email shall comply with the HIPAA Security Transmission of ePHI and HIPAA Privacy Safeguards policies
   c. PPMOK must have a mechanism in place to decrypt any ePHI that it encrypts or has encrypted

5. PPMOK shall implement hardware, software, and/or procedural mechanisms that record for examination the User activity in its Information Systems that contain ePHI. Reviews shall be handled in accordance the HIPAA Security Audits Policy.

6. PPMOK must comply with any other policies designed to protect ePHI.

III. REFERENCES
1. 45 CFR 164.312(c)-(e)
2. HIPAA Security Audits Policy
3. HIPAA Privacy Policy – Safeguards -18
**Contingency Plan for ePHI**

**I. PURPOSE:** To ensure that PPMOK is prepared for emergencies or disasters such that ePHI is protected and available, and the PPMOK is able to continue providing services, as appropriate.

**II. POLICY:** PPMOK, in consultation with IT and the HIPAA Compliance Officer, shall establish and implement a contingency plan consisting of policies and procedures for responding to an emergency or other event that damages its systems that contain ePHI.

**III. PROCEDURE:** PPMOK shall establish, document, and implement a contingency plan that must include, at a minimum, the following:

1. A Data Back-up Plan that will make it possible to retrieve exact copies of PPMOK’s ePHI.

2. If PPMOK maintains all ePHI on its secure servers, it may rely on IT’s data back-up plan to comply with this requirement.

3. If PPMOK maintains ePHI on its own servers, it may model its plan on IT’s plan or develop its own.

4. A Disaster Recovery Plan and services that will make it possible to restore the PPMOK’s lost data. Disaster Recovery Plans, at a minimum, should include the following:
   a. The conditions for activating the Disaster Recovery Plan
   b. Business, infrastructure, and resource requirements for the Plan
   c. Identification and definition of Workforce Member roles and responsibilities in the Plan, as well as contact information
   d. Identification of dependencies on external entities for restoration and requirements for and/or agreements with those entities
   e. Procedures that identify recovery locations and describe the actions to be taken to resume normal operations within required timeframes
   f. The order in which Information Systems or data must be recovered
   g. Allowable or acceptable outage times
   h. Notification and reporting procedures
i. Procedures for allowing appropriate physical access to the Facilities and Information Systems
j. Procedures for obtaining ePHI when normal access is unavailable for business continuity.

5. An Emergency Mode Operation Plan that will enable the PPMOK to perform its critical business functions while still protecting its ePHI.

6. Testing and Revision Procedures to ensure PPMOK’s contingency plan is functioning and appropriate. These procedures should include, at a minimum:
   a. The cycle and scope of tests
   b. The training necessary for those with assigned responsibilities
   c. The types of tests involved (e.g., exercise, walk-through, real operational scenario), based on acceptable business impact for testing.

7. An Applications and Data Criticality Analysis that assesses how critical PPMOK’s ePHI application is and whether it is sufficiently addressed in the contingency plan.

8. Emergency Access Procedures to allow authorized individuals to access Facilities that store ePHI and Information Systems to support the recovery and response efforts of the contingency plan.

9. PPMOK should maintain off-premises a list of emergency contacts that may assist in these efforts, such as Site Support, IT, and the HIPAA Compliance Officer.

10. PPMOK shall assist the HIPAA Compliance Officer in developing a contingency plan and ensure the plan complies with HIPAA Security Rules policy.

IV. REFERENCES:

1. 45 CFR 164.308(a)(7)
2. 45 CFR 164.310(a)(2)(i)
I. PURPOSE: To provide for training regarding PPMOK’s HIPAA Security Policies.

II. POLICY: Personnel shall take PPMOK’s HIPAA Security training annually. Additionally, training shall be provided by the HIPAA Compliance Officer within a reasonable period of time after material changes to HIPAA or PPMOK’s policies and procedures.

III. PROCEDURE:

Program. The HIPAA Compliance Officer shall direct the methods and manner in which training will be accomplished.

Materials. Training materials should include a test to demonstrate understanding of the information presented. Training must be completed according to the standards in this Policy in order for the training requirement to be satisfied.

1. The training program shall also include periodic reminders and updates related to HIPAA Security policies, including but not limited to:
   a. Procedures for guarding against, detecting, and reporting malicious software.
   b. Procedures for monitoring log-in attempts and reporting discrepancies.
   c. Procedures for creating, changing, and safeguarding passwords.

Tracking. PPMOK shall ensure its employees receive training according to its Security Policies.

1. The supervisor of PPMOK shall work with the HIPAA Compliance Officer to ensure that training is accomplished according to company Security Policies.

2. Training will be tracked by using suitable software or other recordkeeping method.

Timing. Each new employee must complete PPMOK’s training as provided below.
1. **Regular Employees** must complete HIPAA Security training within 30 days of becoming an employee. PPMOK must also provide a review of their Security policies and procedures as soon as reasonably possible.

2. **Temporary Employees** must complete PPMOK’s HIPAA Security training if they are expected to work for PPMOK for more than 5 consecutive days. Training must be completed on or before the 6th day of providing services to PPMOK and may be completed online or on a printed version of the online course. Documentation of training must be maintained by PPMOK. In addition, it must provide a review of its relevant HIPAA Security policies as soon as reasonably possible.
   a. Temporary employees providing fewer than 6 consecutive days of service may be required to take Security training. PPMOK must provide these individuals a review of applicable Security policies and procedures as soon as reasonably possible.
   b. Temporary Employees are required to execute PPMOK’s Confidentiality Agreement (available on the website). PPMOK shall maintain that Agreement for at least six (6) years, or for as long as required by other PPMOK policies.

3. **Others** - PPMOK must contact the HIPAA Compliance Officer to determine the training requirements for any other individuals.

**Material Changes.** The HIPAA Compliance Officer will provide training to those workforce members whose job functions are affected by a material change in Security Policies within a reasonable period of time after the change becomes effective.

**Sanctions.** Employees who fail to complete the training are subject to sanctions pursuant to the Sanctions policy. Temporary employees, trainees and others who fail to complete annual training will not be permitted to provide services to or continue training at PPMOK.

**Documentation.** Documentation regarding training must be maintained by the Compliance Officer for at least six (6) years.

**IV. REFERENCES:**

1. 45 CFR 164.308(a)(5)
2. HIPAA Privacy Policy
3. Training Security Policy
4. Sanctions

---

24 PPMOK should give consideration to the length of temporary employment or other position when determining how soon after the first day the individual must complete the training.
I. PURPOSE: To provide for notification in the case of breaches of unsecured ePHI. For purposes of these requirements, “unsecured ePHI” means ePHI that is not secured through the use of approved technologies or methodologies that render ePHI unusable, unreadable, or indecipherable to unauthorized individuals.

II. POLICY: PPMOK’s HIPAA Compliance Officer will implement reasonable and appropriate technologies and methodologies designed to secure ePHI from unauthorized Disclosure. This Policy establishes the requirements regarding the protection of ePHI that PPMOK must comply with and the notification that must occur in the event of a Breach of unsecured ePHI.

III. PROCEDURE: The PPMOK supervisor, in coordination with the HIPAA Compliance Officer, shall be responsible for compliance with this Policy.

Methods of Protection: Either of the following methods may be used to secure ePHI and make it unusable, unreadable, or indecipherable to unauthorized individuals.

1. Encryption: PPMOK will comply with the encryption technologies and methodologies implemented by the HIPAA Compliance Officer to enhance the protection of ePHI.
2. Destruction25: PPMOK will comply with the destruction techniques implemented by the HIPAA Compliance Officer that render ePHI unusable and/or unreadable in any format.
3. For additional information on the guidelines and standards of encryption and destruction methods of ePHI, contact the HIPAA Compliance Officer

Notification of Breach: If a Breach of ePHI is suspected or discovered, the HIPAA Compliance Office must be notified immediately. The Officer will determine, using the Breach Notification

25 Refer to Information Technology Electronic Data Disposal Policy for destruction requirements of ePHI. Refer to Safeguards policy, for destruction requirements of paper records containing Protected Health Information
Reporting Process, whether and when a notice to the individual, the media, and/or HHS is appropriate and, if so, the content of the notice.

1. In the event a Breach of unsecured ePHI, PPMOK may be required to notify each individual whose unsecured ePHI has been, or is reasonably believed to have been, inappropriately accessed, acquired, Used, or Disclosed. The HIPAA Compliance Officer shall make such notice according to the requirements of HIPPA, as provided in Privacy 34, Breach of Unsecured PHI.

**Tracking:** The HIPAA must maintain a log of breaches of unsecure ePHI. PPMOK shall promptly notify the HIPAA Compliance Officer of each breach.

1. The HIPAA Compliance Officer shall maintain a log of all reported breaches of unsecure ePHI and shall submit required reports of such to the Secretary of HHS annually, as Required by Law.

**IV. REFERENCES:**

1. Department of Health and Human Services Breach HIPAA FAQ Page:
3. 45 CFR Part 164.308
4. NIST SP 800-111 “Guide to Storage Encryption Technologies for End User Devices” and SP800-88 “Guidelines for Media Sanitization” and related updates or revisions
5. Oklahoma State Breach Notification law
6. HIPAA Privacy Policy, Breach of Unsecured Protected Health Information
**Subject**: Business Associates and ePHI

---

**Policy #:** Security -10  
**Approved:** May 23, 2014

**Effective Date:** May 30, 2014  
**Revised:**

**Next Review Date:** July 31, 2014  
**Reviewer:**

---

**I. PURPOSE:** To establish requirements regarding Uses and Disclosures of ePHI to or by Business Associates.

**II. POLICY:** PPMOK may Disclose ePHI to a Business Associate and may allow a Business Associate to create, receive, maintain, or transmit ePHI on its behalf, if PPMOK confirms (through the HIPAA Compliance Officer) that PPMOK has executed a Business Associate Agreement (BAA) with the Business Associate which contains language requiring the Business Associate to appropriately safeguard the ePHI in compliance with HIPAA.

1. If a PPMOK Workforce Member knows of a pattern of activity or practice of a Business Associate that constitutes a material breach or violation of the Business Associate’s obligation under the BAA, it must take reasonable steps to cure the breach or end the violation. The HIPAA Compliance Officer shall be notified by PPMOK which has any concern regarding any Business Associate as to HIPAA compliance. If such steps are unsuccessful or cure is not possible, PPMOK shall contact the Officer for assistance in terminating the Agreement. If termination is not possible, the Officer shall determine whether to report the problem to the Secretary of the Department of Health and Human Services.

**III. PROCEDURE:** the procedures for using Business Associates to create, receive, maintain, or transmit the ePHI are found in the privacy policy titled “Business Associates.”

**IV. REFERENCES:**

1. 45 C.F.R. 164.502(e); 45 C.F.R. 164.530
2. 45 C.F.R 308(b); 45 C.F.R. 164.312(a)
3. Privacy Policy--Business Associates
I. PURPOSE: To ensure Workforce Member access to ePHI is appropriate and complies with the minimum necessary rule under HIPAA.

II. POLICY: Before access to ePHI can be established for a User, PPMOK must authorize the User for the appropriate level of access for the User’s job responsibilities.

III. PROCEDURE:

1. Access Authorization: Using the Role-Based Access Worksheet (available through the HIPAA Compliance Officer), the supervisor of PPMOK must designate in writing the appropriate level of access to ePHI for each employee. This must occur upon employment/appointment and when access requirements change.

2. The HIPAA Compliance Officer, in consultation with PPMOK, will resolve any conflicts or discrepancies regarding the level of access to ePHI requested.

3. Workforce Members who are directly involved in a patient’s Treatment (e.g., physicians and nurses) may have access to the patient’s entire PHI. Personnel who are not directly involved in a patient’s Treatment should generally not have unlimited access to a patient’s PHI -- access by these individuals is governed by the minimum necessary rule.

4. It is a violation of the minimum necessary rule for a Health Care Provider to access the PHI of patients with whom the provider has no Treatment relationship, unless for approved Research purposes or as permitted by the HIPAA Privacy policy, Uses and Disclosures – General and Authorization. This includes accessing the PHI of family members, friends or acquaintances, etc.

5. The PPMOK supervisor shall, in conjunction with the HIPAA Compliance Officer, be responsible for establishing, modifying, and removing access to the ePHI maintained in
the PPMOK’s system. This individual shall also maintain the Role-Based Access Worksheet for each PPMOK Workforce Member.

6. Once access to ePHI has been granted, the HIPAA Compliance Officer will keep the approved Role-Based Access Worksheet on file for a minimum of six years from the time access is terminated. A copy of the Worksheet for employees must be sent to Human Resources for inclusion in the employee’s file.

7. All accounts belonging to the terminated employee shall be disabled immediately and remain disabled for a period of 30 days. After 30 days, the accounts shall be deleted from PPMOK’s system.

8. Any facility manager, business manager, and supervisor can request via email to the HIPAA Compliance Officer that accounts of employees who have been terminated under less than desirable conditions be disabled. These accounts will be disabled immediately and remain disabled for a period of 30 days. After 30 days, the accounts shall be deleted.

9. Requests for access to disabled accounts must be made to Human Resources.

10. Reviews of User access levels will be conducted during the HIPAA compliance audits of PPMOK. The facility supervisors shall also verify periodically, such as during performance evaluations, that User access is appropriate.

IV. REFERENCES:

1. 164.308(a)(4)(ii)(B); 164.308(a)(4)(ii)(C); 164.316(b)(2)(i)
2. HIPAA Privacy Policy -, Minimum Necessary Rule
I. PURPOSE: To describe the Technical Safeguards that must be in place to protect PPMOK’s ePHI from unauthorized Access and Use.

II. POLICY: PPMOK, in coordination with IT and the HIPAA Compliance Officer, shall have in place Technical Safeguards to protect the ePHI it maintains on its Information Systems from unauthorized Access or Use via access and audit Controls.

III. PROCEDURE: As part of its Technical Safeguards, PPMOK shall comply with or provide for the following:

1. Information Technology Password Management Policy and Standards
   a. Each Workforce Member must have and use unique identification when accessing Information Systems;
   b. Shared devices shall be configured to require unique User identification.

2. Emergency Access Procedures: PPMOK management or IT must have the ability to Access ePHI on a particular Information System (such as a User’s computer) in the event of an emergency.

3. Computer Logoff/Lock Policy: HCC administration shall enforce the following requirements for computer lock and logoff:
   a. Lock: Workforce Members must manually lock or logoff a computing device or application when leaving that device or application unattended.
   b. Automated Lock or Logoff: All computing devices and applications must be secured with either a password-protected screen saver or automatic logoff that will take effect after no more than 45 minutes of inactivity.

4. Encryption and Decryption of ePHI
a. ePHI must be encrypted when being transferred between and stored on Information Systems external to PPMOK.

b. ePHI sent via email shall comply with the HIPAA Security Transmission of ePHI and the HIPAA Privacy Safeguards policies.

c. PPMOK must have a mechanism in place to decrypt any ePHI that it encrypts or has encrypted.

5. PPMOK shall, in coordination with IT and the HIPAA Compliance Officer, implement hardware, software, and/or procedural mechanisms that record for examination the User activity in its Information Systems that contain ePHI. Reviews shall be handled in accordance the HIPAA Security Audits and related audit policies.

6. PPMOK must comply with any other IT policies designed to protect Information Systems that maintain ePHI.

IV. REFERENCES:

1. 45 CFR 164.312(a) –
2. Information Technology Password Management Policy and Standards
3. Information Technology Transmission of Sensitive Data Policy
4. Information Technology Computer Logoff/Lock Policy
5. Information Technology Activity (Log) Review Policy
6. HIPAA Security Audits Policy
7. HIPAA Privacy Policy – Privacy Compliance Audits
8. HIPAA Privacy Policy - Safeguards
I. PURPOSE: To ensure that Workstations and other computer systems that access, store or transmit ePHI are used in a secure and appropriate manner.

II. POLICY: PPMOK and its Workforce Members (“Users”) who use electronic computing devices that access, store, or transmit ePHI, such as desktops, laptops, smart phones, flash drives, and, tablets (“Workstations”) shall comply with the following policies.

1. Workstation policy:
   a. Workstations shall not be accessible by persons who do not have a unique username and password issued by PPMOK.
   b. Workstations shall be protected with current anti-virus software selected and installed by IT.
   c. Workstations should be set to receive automatic update notifications regarding operating system software and antivirus software.
   d. Workstations shall be protected by a firewall that denies all unnecessary incoming network connection attempts.

2. Proper Use of Workstations
   a. Users shall observe the minimum necessary standard at all times (i.e., use Workstations to Access only that ePHI needed to Access to perform a job-related function).
   b. Users shall not attempt to exceed their Access or attempt to Access any network, system, application, or data to which they have not been granted access.
   c. Each User shall be informed and asked whether he or she understands that Workstation use may be audited at the discretion of the HIPAA Compliance Officer to confirm compliance with PPMOK policies.
   d. Users shall not download any software, applications, documents, etc. on PPMOK Workstations without prior authorization of IT. An administrator login and
password shall be required to make material changes to any program, hardware, or to download any type of software onto a PPMOK workstation.

e. Workstations shall not be used for personal matters or for recreational surfing of the Internet.

f. Users shall not open suspicious emails, and shall promptly notify IT regarding any suspicious emails received.

3. Workstation Locations

a. Users shall secure Workstations or shall locate them in areas that can be secured when they are not attended.

b. Users shall position Workstation monitors away from view of those in common areas or install privacy screens to prevent unauthorized observation.

c. Users must return the screens on Workstations to a password-protected screen saver or login screen when the Workstation will be unattended.

4. Storing ePHI on Workstations

a. Users shall not store ePHI on unencrypted Workstations.

b. ePHI should be stored on servers in a secure enterprise data center or on encrypted Workstations.

c. Each User is responsible for the security of his/her Workstation and the ePHI stored on the Workstation.

d. Users must comply with all PPMOK Security Standards, such as password protection.

e. Only encrypted portable computing devices may be used for PPOK business, regardless of whether the device is owned by PPMOK or the User.

5. Theft or Loss

a. Users must immediately report the theft or loss of any Workstation containing ePHI (including those owned by the individual) to the HIPAA Compliance Officer and HIPAA Security Officer, as well as to any person designated by PPMOK to receive such reports, so that mitigation and reporting options can be considered and implemented as soon as possible. (See HIPAA Security policy, Breach of Unsecured PHI.)

b. Users must cooperate with those individuals who are investigating the theft or loss of Workstations containing ePHI and/or mitigating any related harm.

6. Updates and Security

a. Users shall cooperate with IT to ensure Workstations are part of a patch or vulnerability management system.

b. Each User has a unique User authentication.
c. PPMOK shall not put into service any portable computing device that is not encrypted, in accordance with C(4) above.

d. PPMOK shall require their Workforce Members to password-protect their devices that connect to its network or other system containing ePHI.

IV. REFERENCES:

1. 45 CFR 164.308(a)(1)(ii)(B)
2. 45 CFR 164.310
3. HIPAA Privacy Policy, Safeguards -18
4. HIPAA Security Policy, Breach of Unsecured Protected Health Information
5. HIPAA Privacy Policy, Minimum Necessary Rule – 21
Working Off-Site

I. PURPOSE: To ensure HIPAA privacy and security policies are followed, and all PHI is protected when employees perform work off-site.

II. POLICY: Working off-site and working with portable computing devices and media carry greater information security risks than working in our facility. Therefore, when used off-site, stationary workstations, portable computing devices (e.g., laptop computers, PDAs, and smartphones), and portable electronic or other media used to store and/or access this organization’s confidential data must be protected from unauthorized access, disclosure, damage, or loss through heightened administrative, physical, and technical controls.

1. To ensure that individuals recognize the increased risk and their responsibility, individuals who work off-site with this organization’s confidential information, even occasionally, must sign a Working Off-Site Security Agreement. Further, if work is performed in a fixed location, such as a home or small office, individuals must agree to permit an on-site review, if and when this organization undertakes such reviews, with advance notice, to verify compliance with security policies and procedures.

2. This policy is intended to supplement other information security policies for the special case of working off-site with both portable and non-portable equipment and media.

3. Personally owned workstations, portable computers, and portable storage media used for our business purposes off-site are subject to specific risks not present on-site. Portables are at greater risk of loss and theft than non-portable items. Personally owned workstations used for business are typically also used for personal reasons that could compromise this organization’s data and systems. Either could be used in a home or public setting, where numerous physical and technical risks exist. Therefore, when they contain confidential information, that information could be compromised by unauthorized access. It could also be altered or destroyed through unauthorized actions.
There is heightened risk to the data on the device or media. Also, if the device is used to access this organization’s network and other protected resources, the security of all information assets could be at greater risk. Unsecure devices can be used for unauthorized access (e.g., when a password is stored on a laptop computer or no device authentication is required) and can introduce malware. Hence, the additional security controls in this policy are appropriate and necessary to contain the risks.

**III: SCOPE:** This policy applies to our workforce and any third parties who are authorized to have or to access any information this organization designates as confidential or highly confidential (e.g., PHI employee records) and who work off-site using workstations or portable computers to access or store our confidential data and/or who remove confidential data from this organization.

1. This policy applies both when the organization owns the device or medium and when it does not, as long as our confidential data are accessed through or stored on the device or medium.
2. This policy applies to any user computing device. This includes workstations, such as personal computers, in homes. It includes portable computers, such as, but not limited to, laptop computers, tablets, and handheld devices (e.g., PDAs, pagers, and smartphones with storage and processing capability).
3. This policy also applies to portable media of all forms, including paper. Examples of portable electronic media include external hard drives, CDs, MP3 players, SD cards, and USB drives.
4. This policy (particularly the inventory, encryption, and physical security controls) also applies to portable electronic storage, including backup tapes and cartridges, and records being archived.

**IV: PROCEDURE:**

1. **Inventory of Portable and Other Computing Devices and Electronic Media**

2. The HIPAA Compliance Officer and IT will create and maintain an inventory of computing devices used to access and/or store this organization’s confidential data off-site. The inventory includes both organization-owned and personally owned devices. Devices include desktop workstations, laptop computers, tablets, smartphones, and any other user-computing device. Individuals are responsible for reporting new devices, replacements, and inventory information changes promptly. IT will also track portable electronic media, such as USB drives.

3. The inventory will give the HIPAA Compliance Officer information about how these devices are being used off-site with respect to confidential data. Based on review of
this information, and/or on new risks, the Compliance Officer may mandate additional security controls and specific security software.

4. Upon termination, or when the computing device or medium is no longer needed, organization-owned devices and media must be returned to the organization, wiped clean, and returned to inventory. Upon termination, personally owned computing devices and media must be wiped clean of organization data and organization-licensed software, if any, and the user must signed a statement acknowledging that all data and software have been removed according to organization secure erase standards. Organization-issued storage media must be returned, physically destroyed, or wiped clean using acceptable secure erase software.

5. Authorization and Acknowledgement: Individuals must be authorized in writing by management prior to working off-site if doing so entails a remote connection to the organization’s network or if it entails accessing and/or storing any confidential data on an off-site or portable device or media. Note that authorization is required even if there is no need for a remote connection to this organization’s private network.

6. Individuals must sign an acknowledgement of their security responsibilities and to permit announced site visits for a security review, if and when the organization performs them. Additionally, individuals must agree to permit this organization to remotely lock and/or wipe contents from portable devices with this capability when a risk exists. This may include, but is not limited to, when the device is stolen and when there are three consecutive unsuccessful logon attempts. Finally, individuals must agree that computing devices used for work purposes must not be shared with others, regardless of device ownership.

7. User Identification, Authentication, and Access Control Access to personal computing devices used for this organization’s work requires a unique user ID. Exceptions may be permitted for certain devices, such as smartphones. The device may not be shared with another individual unless approved by this organization.
   a. Access to the device requires at least one form of user authentication, such as a password, PIN, or fingerprint. Passwords and other forms of authentication must meet organization standards. Passwords that are also used as encryption keys must be longer passphrases (e.g., 20 characters) that meet organization standards. Passwords and passphrases are secret; they may not be shared and they may not be saved on the device.
   b. Devices containing confidential data or that are used to access confidential data may not be left logged on and unattended. The user must log off or “lock” the device so that re-authentication is required to use the device.
c. Portable devices, such as laptop computers, tablets, and smartphones used for business purposes, must be centrally controlled by this organization to permit, for example, remote locking and/or wiping in case of loss or theft. This applies regardless of device ownership.

8. Inactivity Timeout: Devices must be configured to automatically time out or terminate the session after forty-five minutes (45). Note that this is intended as a safety net and does not relieve the user of the responsibility to lock or log off before leaving a device unattended.
   a. Remote access to the organization network will time out after a designated period of fifteen minutes of inactivity. This may be set in a VPN connection or SSL connection through a website where user re-authentication will be required for an application to continue.

9. Software: The HIPAA Compliance Officer and IT will develop and maintain configuration standards to be followed. Users generally are not permitted to modify organization-owned devices, and they are required to maintain personally owned devices in accordance with this policy.
   a. Downloading software apps from the Internet should be done with great care, particularly on smartphones, and only when the source is reliable. IT will maintain a list of approved applications.
   b. Virus protection and antimalware software must be installed on devices, updated promptly when security updates are available, and configured to scan vulnerable components. Use of a personal device firewall is also required. Security updates to operating systems, browsers, and applications must be promptly applied to devices.
   c. File sharing software must not be installed or enabled.

10. Encryption: All portable computing devices (e.g., laptop computers) and portable electronic media (e.g., USB drives) used for organization work must be encryption-enabled to protect stored organization confidential data. Consult IT for assistance.
   a. Only National Institute of Standards and Technology (NIST)–endorsed algorithms, such as AES, may be used. Decryption keys must be stored separately from the device or media and kept confidential. IT will provide key escrow services when appropriate.
   b. When a device is connected to a network (wired or wireless), and any portion of the connection is over the air, the Internet, or a network not under the control of this organization, transmission must be encrypted. This can be accomplished with standard technologies (e.g., IPsec VPN, SSL/HTTPS,
Secure Shell, secure FTP). Wireless networks, including home networks, must be configured with WPA2 or higher.

11. File Backup: If off-site data are unique source data that could not be recreated and are important to this organization’s operations, it must be backed up to a secure file server on the network.

12. Physical Protections: Whether using a desktop computer or a portable device, it should be set up or used in a private area where access to the device is restricted. In all cases, users must be aware of their surroundings and must protect screens from view by others. Devices should have privacy screens (e.g., filters or films) unless the device is a desktop computer in a private office.
   a. Logged-on devices must never be left unattended if anyone else is or may be in the vicinity. Note that disk encryption does not provide protection when the user is logged on.
   b. Portable devices must be kept logged off and physically locked up (e.g., in a locked drawer or locked briefcase) unless they are in use or on one’s person. Media of any type (e.g., electronic, paper) containing confidential information must be locked securely when unattended.
   c. When transporting portable computing devices and/or media containing confidential data, the items must be on one’s person or logged off, locked up, and out of sight. For example, a laptop computer and work papers left in a parked vehicle or a hotel room must be in a locked case and hidden out of sight. Locks are not foolproof, but they are an important deterrent to theft. In vulnerable circumstances, portable devices and media should be kept with the responsible individual.
   d. When portable media in any form are transported by or for a department (e.g., for record archiving, for data backup and restore, and similar purposes), the media must be in a locked case. When media containing confidential data are stored off-site, they must be in locked containers unless an exception is authorized in writing by the HIPAA Compliance Officer.

13. Disposal: When files containing confidential data are no longer needed, follow organization policy and procedures for safely disposing of the information. Seek assistance from IT, if necessary, to thoroughly erase or destroy electronic data. All paper containing confidential data must be cross-cut shredded.

14. Loss or Theft: Users must report the loss or theft of any device or media that may contain confidential information to the HIPAA Compliance Officer within twenty-four (24) hours. This event will be treated as a privacy/security incident to be
immediately triaged and investigated. If appropriate, IT will remotely lock and/or wipe contents from the device.

15. Monitoring and Enforcement: The HIPAA Compliance Officer is responsible for monitoring and enforcing this policy. However, managers and each member of this workforce also share responsibility for ensuring compliance with this policy and reporting violations.

V. REFERENCES:
I. PURPOSE: To establish a process for imposing sanctions in the event PPMOK’s HIPAA Security policies or the HIPAA Security Rules are violated.

II. POLICY: PPMOK will apply sanctions as appropriate against Personnel as well as its Business Associates who fail to comply with its HIPAA Security policies and rules. PPMOK will not impose sanctions against Personnel or Business Associates for:

1. engaging in good faith whistleblower activities related to HIPAA Security issues;
2. submitting a complaint in good faith to the Secretary of the Department of Health and Human Services or other enforcement agency;
3. participating in an investigation regarding HIPAA Security issues; or
4. appropriately registering opposition to a violation of the HIPAA Security policies or HIPAA Security Rules.

III. PROCEDURE: Refer to HIPAA Privacy policy Sanctions, for the procedures for applying Sanctions in the event the HIPAA Security policies or HIPAA Security Rules are violated.

IV. REFERENCES:

1. 45 CFR 164.312(e)
2. HIPAA Privacy Policy, Sanctions