Five Rivers Medical Center, Inc.

2801 Medical Center Drive
Pocahontas, AR 72455

Notification of Security Breach Policy

Purpose:

This policy has been adopted for the purpose of complying with the Health Information Technology for Economic and Clinical Health ("HITECH") Act, (which revised the Health Insurance Portability and Accountability Act of 1996 ("HIPAA")), and the Arkansas Personal Information Protection Act.

Scope:

This policy applies to all members of the workforce, which includes all employees, medical staff, students, contractors, and/or agents, who access or use protected health information and/or personal information of patients.

Definitions:

a) **Breach.** Breach means a use or disclosure of protected health information ("PHI") in a manner not permitted under the HIPAA Privacy Rule, which poses a significant risk of financial, reputational or other harm to the individual whose PHI was breached.

b) **Unsecured PHI.** Unsecured PHI is PHI that is not encrypted, destroyed or otherwise unreadable to unauthorized individuals. For PHI that is encrypted, encryption keys must be stored separately from the PHI. Destruction of paper, film or other hard copy media requires shredding or other measures so that the PHI cannot be read or reconstructed. Destruction of electronic media requires clearing, purging or other measures so that the information cannot be retrieved. Redaction, firewalls and access controls are not sufficient for making PHI secure.

c) **Jurisdiction.** Jurisdiction means a geographic area smaller than a state, such as a county, city or town.

d) **State.** For purposes of this policy, State includes any state, Washington D.C., Puerto Rico, the Virgin Islands, Guam, American Samoa and the Northern Mariana Islands.

PROCEDURE

Discovery of a Breach:

All members of the workforce must promptly notify the Compliance Officer upon discovery of a possible Breach. The Compliance Officer will then perform an analysis to determine whether

the acquisition, access, use or disclosure is impermissible under the HIPAA Privacy Regulations or falls under one of the exceptions. If not, the Compliance Officer will presume a Breach has occurred unless it can be demonstrated there is a low probability that the protected health information has been compromised based on a risk assessment that includes consideration of the following factors:

a) The nature and extent of the protected health information involved, including the types of identifiers that were disclosed;

b) The person or entity to whom the disclosure was made;

c) Whether the protected health information was actually acquired or viewed; and

d) The extent to which the risk to the protected health information has been mitigated.

If it is determined that there is a low probability that the protected health information has been compromised, no Breach has occurred.

Documentation of all risk assessments will be maintained for at least six (6) years. Documentation must include whether or not the incident that triggered the risk assessment was determined to be a Breach, and the reason for the determination.

If an incident is determined to be a Breach, measures will be taken as soon as possible to reduce the effects of the Breach. These measures will be based on the risk assessment and may include, but are not limited to:

a) Contacting the affected individual(s)
b) Notifying law enforcement
c) Obtaining satisfactory assurances that the PHI will not be further disclosed
d) Updating or enhancing security measures
e) Changing passwords or security codes

A Breach is considered discovered when the incident is discovered, not when there is a conclusion that the use or disclosure constitutes a Breach.

<u>Exceptions to Breach</u>:

1. The unintentional access or use of PHI by an employee who is acting in good faith and within their scope of employment is not a Breach provided that no further disclosure occurs.

   As an example, if a billing employee opened an email containing PHI that was mistakenly sent to him, and he notifies the sender of the mistake and deletes the email, no Breach has occurred. However, access of PHI by an employee for the purpose of finding out information about a friend would constitute a Breach because this access was not within the scope of employment.

2. The inadvertent disclosure of PHI from one authorized person to another authorized person at the covered entity or business associate is not a Breach.

   This exception applies to inadvertent disclosures by individuals who are otherwise authorized to access PHI, provided that the PHI is not further disclosed except as permitted under the Privacy Rule. It applies to inadvertent disclosures to individuals in organized health care arrangements in which covered entities participate (such as a hospital and its medical staff). It also applies when the disclosure is made between separate facilities owned by the same entity.

3. An unauthorized disclosure is not a breach if the individual who received the information could not be expected to be able to keep or remember the information.

   As an example, if documents containing PHI were inadvertently mailed to the wrong person, but returned undeliverable and unopened, no Breach will have occurred.

For all three exceptions, documentation of why the exception applies is required. This documentation must be maintained for six (6) years.

Notice to Individuals:

When it is determined that a Breach has occurred, all affected individuals will be notified as soon as reasonably possible, but at least within sixty (60) days after discovery of the Breach, unless a delay is requested by law enforcement.

If law enforcement states in writing that providing notice would impede a criminal investigation or damage national security, notice may be delayed for the time period specified by law enforcement.

If law enforcement states orally that a delay is necessary for the reasons listed above, the statement and the identity of the law enforcement official will be documented. Notice will not be delayed for longer than thirty (30) days, unless a written statement is provided during that time.

Notice will be written in clear language and will be translated into other languages or formats, such as Braille or audio when necessary. The content of the Notice will include:

a) A brief description of the incident, including the date of the Breach and the date of discovery, if known;

b) A description of the types of information involved;

c) A brief description of what is being done to investigate the Breach, mitigate harm (such as information on how to contact credit card companies, or credit bureaus or how to obtain credit monitoring services) and protect against further Breaches;

d) Any steps individuals should take to protect themselves from potential harm resulting from the Breach; and

e) Contact procedures for questions or to obtain additional information, including a toll-free number, email address, website, or postal address.

Notice will be sent via first-class mail to the last known address of the affected individual(s). If the individual is a minor or is incapacitated, notice will be provided to a personal representative. If contact information is insufficient or out-of-date, or if any notices are returned undeliverable, substitute notice will be provided.

Substitute notice will be provided as soon as reasonably possible after becoming aware that contact information is insufficient. Substitute notice will contain all of the elements listed above.

If contact information for providing written notice is insufficient or out-of-date for less than ten (10) individuals, substitute notice may be provided by telephone or email.

If contact information is insufficient or out-of-date for more than ten (10) individuals, notice will be provided on the website, or through newspapers, radio or television in the geographic areas where the affected individual(s) likely reside. This notice will include a toll-free phone number that individuals can call to find out if their unsecured PHI was included in the Breach.

Any notice posted on the website will be located on the home page or through a hyperlink for ninety (90) days. The notice will be prominent and will include the elements listed above.

If urgent notice is required, such as when imminent misuse of unsecured PHI is likely, notice may be sent by telephone or email in addition to written notice.

If an affected individual is deceased, notice will be sent to the last known address of the next of kin or personal representative, if known. Substitute notice is not required for decedents when contact information for the next of kin or personal representative is unknown or out-of-date.

Notice to the Media:

If a Breach involves more than 500 residents of a state or jurisdiction, notice will be provided through newspapers, radio or television serving the area. As an example, if a Breach involved more than 500 residents in one city, notice could be provided to a newspaper serving that city. If a Breach involved residents across an entire state, notice could be provided to a newspaper serving the entire state.

Notice to the media is different than *substitute notice* to the media because this type of notice is in addition to, but not a substitute for, individual notice.

Notice to the media will be provided as soon as reasonably possible, but at least within sixty (60) days after discovery of the Breach. This notice will include the same information included in the individual notices.

If a Breach involves multiple states or jurisdictions, media notice will be provided if the Breach affects more than 500 residents in any one state or jurisdiction. As an example, if a Breach involves 200 individuals in one state, 100 individuals in another state, and 250 individuals in yet

another state, media notice is not required because not more than 500 individuals in one state were involved. However, individual notice will still be provided as described above.

Notice to the Secretary of Health and Human Services:

If a Breach involves 500 or more individuals (regardless of whether they are residents of one particular state or jurisdiction), the Secretary of HHS will be notified at the same time and in the same manner as the individuals are notified Instructions for submission of this notice can be found on the HHS website.

Documentation of Breaches involving less than 500 individuals will be maintained and submitted to the Secretary annually. Submission must occur no later than sixty (60) days after the end of each calendar year. This documentation will be maintained for six (6) years, and will also be made available to the Secretary upon request.

Unauthorized Acquisition of Personal Information:

In the event of an unauthorized access of computer data that contains personal information, but that is not considered a Breach of unsecured PHI, affected individuals will be notified as required by state law, following consultation with legal counsel.

For purposes of this section, "personal information" means an individual's first name or first initial and his or her last name, in combination with any of the following information, when either the name or the data element is not encrypted or redacted:

a) Social security number;

b) Driver's license number or Arkansas identification card number; or

c) Account number, credit card number, or debit card number in combination with any required security code, access code, or password that would permit access to the account.

Implementation:

All members of the workforce, including all employees, medical staff, students, contractors, and/or agents, who access or use PHI and/or personal information of patients, will be educated on this policy, the importance of reporting any potential Breach of unauthorized access and the consequences for failure to report.

Failure to comply with this policy shall result in sanctions, up to and including termination of employment.

All reports or complaints regarding this policy may be submitted to the Compliance Officer. No retaliation shall be taken against any individual who makes a report or files a complaint pursuant to this policy.