ACCOUNTING OF DISCLOSURES OF PROTECTED HEALTH INFORMATION

This is an accounting under the Privacy Rule of the Health Insurance Portability and Accountability Act of 1996 and the regulations promulgated thereunder (as the same may be amended from time to time, collectively, "HIPAA").

Under HIPAA, you have the right, with some exceptions, to receive an accounting of disclosures of protected health information made by us and our business associates. The first accounting in any 12-month period is without charge to you. Other accountings requested by you within the same 12-month period may be subject to a reasonable, cost-based fee. The accounting you requested is set forth below.

ACCOUNTING

A. Our Disclosures

Patient Name	Date of Disclosure	Name and (if Known) Address of Recipient	Protected Health Information Disclosed	Purpose of Disclosure

B. Our Business Associates' Disclosures

Patient Name	Date of Disclosure and by Whom	Name and (if known) Address of Recipient	Protected Health Information Disclosed	Purpose of Disclosure

This accounting has been prepared in accordance with the above-referenced Privacy Rule and is being furnished to you in compliance with our obligations under HIPAA.

If you have any questions, please contact the Hospital's Privacy Officer.

Name of Covered Entity: [Community Hospital, LLC/TPG Hospital, LLC d/b/a Northwest Surgical Hospital]

Date of Request:_____

Date of Accounting:_____

_____ _____

Privacy Officer *Date*

AUTHORIZATION TO USE OR DISCLOSE PROTECTED HEALTH INFORMATION

Provider:

Community Hospital	CH Outpatient Therapy Quail	CH Outpatient Therapy North	CH Outpatient Therapy South	CH Outpatient Therapy Hand
3100 S.W. 89th Street	14024 Quail Pointe Drive	801 N. W. 63rd Street	10001 S. Western Ave.	10001 S. Western Ave.
Oklahoma City, OK 73159	Oklahoma City, OK 73134	Oklahoma City, OK 73116	Oklahoma City, OK 73139	Oklahoma City, OK 73139
(405)602-8100	(405)340-2025	(405)879-9997	(405)691-5434	(405)427-3752

Patient Name: _____ **Date of Birth:** _____

Recipient & Purpose of Request:
I authorize Provider to disclose my protected health information to the following ("Recipient"): _____
at this address _____
for this purpose: _____

I authorize Provider to use or disclose the following protected health information of the Patient described above to Recipient described above in a manner consistent with this authorization (check all that apply):

☐ Entire medical record concerning this patient (excluding psychotherapy notes, if any).

☐ Entire billing record concerning this patient.

☐ Medical record concerning this patient for the following date(s) of service: _____

☐ Billing record concerning this patient for the following date(s) of service: _____

☐ Other: _____

I understand the following:

- Protected health information is health information that identifies me. The purpose of this authorization is to allow Provider to share my protected health information as set forth above.
- I understand that this authorization is voluntary and that I have the right to refuse to sign this authorization. If I refuse, my protected health information will not be used or disclosed by Provider except as otherwise permitted by law. Provider may not condition treatment on my providing this authorization for use or disclosure of my medical information. If I refuse to sign this authorization, I will still be eligible to receive medical services from Provider.
- Subject to certain exceptions, I have the right to revoke this authorization at any time by sending a letter to Provider which gives my name, the date I signed this authorization, and states that I revoke the authorization to use my protected health information. The letter will not affect any actions taken in reliance of my previous authorization.
- This authorization may result in Provider disclosing my medical information to a recipient who could possibly later use or disclose the information without my authorization. Provider cannot control re-disclosure by Recipient.
- I may inspect or copy the information that will be disclosed or used for the purposes set forth in this authorization. I will receive a signed copy of this authorization form and may contact Provider to get a copy if I do not have one.
- **Protected health information authorized for release may include records that indicate the presence of or regarding treatment of HIV/AIDS, sexually transmitted disease, and drug and/or alcohol abuse.**

_____ _____
Signature of Patient or Patient's Representative Date

_____
Printed Name of Patient or Patient's Representative

Description of Representative's authority (attach documentation):
□ Parent of a minor □ Legal guardian
□ Power of attorney
□ Other: _____

This authorization is only effective if it is signed and dated. Unless I revoke this authorization prior to expiration, this authorization expires on _____ (or if this is left blank, one year after the date it is signed).

Community Hospital, LLC *Effective March 1, 2014*
TPG Hospital, LLC d/b/a Northwest Surgical Hospital

HIPAA BREACH NOTIFICATION POLICY

Purpose: To provide guidance to Community Hospital, LLC and TPG Hospital, LLC d/b/a Northwest Surgical Hospital (collectively referred to herein as "Hospital") for breach notification when an unpermitted or unauthorized access, acquisition, use and/or disclosure of patient protected health information occurs.

Breach notification will be carried out in compliance with the HIPAA Rules (45 CFR Parts 160 & 164) as well as any other federal or state notification law.
(See www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/index.html)

Attachments:

- Sample Notification Letter to Patients
- Sample Media Notification Statement/Release
- Sample Breach Notification Log

Definitions:

Access: Means the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource.

Breach: Means the acquisition, access, use, or disclosure of Protected Health Information ("PHI") in a manner not permitted under the HIPAA Rules which compromises the security or privacy of the PHI.

Breach excludes:

1. Any unintentional acquisition, access or use of PHI by an employee of Hospital or other workforce member or person acting under the authority of Hospital or a business associate of Hospital, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the HIPAA Rules.
2. Any inadvertent disclosure by a person who is authorized to access Hospital's PHI to another person authorized to access Hospital's PHI, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the HIPAA Rules.
3. A disclosure of PHI where Hospital or its business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

Disclosure: Disclosure means the release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information.

Individually Identifiable Health Information: Information collected from an individual that is (1) created or received by Hospital; (2) 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; and (3) identifies the individual (using any of the patient identifiers listed in 1-19 below); or with respect to which there is a reasonable basis to believe the information can be used to identify the individual. To be individually identifiable information and subject to HIPAA, the information must satisfy all three of these requirements.

Patient identifiers include the following:

1. Name
2. Address
3. Phone Numbers
4. Fax Number
5. Dates (birth, death, admission, discharge, etc.)
6. Social Security Number
7. E-mail Address
8. Medical Record Numbers
9. Health Plan Beneficiary Numbers
10. Account Numbers
11. Certificate or License Numbers

12. Vehicle Identifiers and Serial Numbers, including license plate numbers
13. Device Identifiers and Serial Numbers
14. Web Universal Resource Locators (URLs)
15. Internet Protocol (IP) Address Numbers
16. Biometric Identifiers, including finger and voice prints
17. Full Face Photographic Images and any comparable images
18. Any other unique identifying number, characteristic, or code
19. Patient's Medical History

Law Enforcement Official: Any officer or employee of an 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 investigate or conduct and official inquiry into a potential violation of law; or prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

Protected Health Information ("PHI"): Protected health information means "individually identifiable health information" (defined above) that is transmitted or maintained in any form or medium, including electronically.

Unsecured PHI: PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of technology or methodology specified by the Secretary of Health and Human Services. PHI is "secured" if the following two requirements are satisfied:

1. Electronic PHI has been encrypted as specified in the HIPAA Rules by the 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 and such confidential process or key that might enable decryption has not been breached. To avoid a breach of the confidential process or key, these decryption tools should be stored on a device or at a location separate from the data they are used to encrypt or decrypt. Either of the following encryption processes meets this standard.

    A. Valid encryption processes for data at rest (i.e. data that resides in databases, file systems and other structured storage systems) are consistent with NIST Special Publication 800-111, Guide to Storage Encryption Technologies for End User Devices.

    B. Valid encryption processes for data in motion (i.e. data that is moving through a network, including wireless transmission) are those that comply, as appropriate, with NIST Special Publications 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations; 800-77, Guide to IPsec VPNs; or 800-113, Guide to SSL VPNs, and may include others which are Federal Information Processing Standards FIPS 140-2 validated.

2. The media on which the PHI is stored or recorded has been destroyed in the following ways:

    A. Paper, film, or other hard copy media has been shredded or destroyed such that the PHI cannot be read or otherwise cannot be reconstructed. Redaction is specifically excluded as a means of data destruction.

    B. Electronic media have been cleared, purged, or destroyed consistent with NIST Special Publications 800-88, Guidelines for Media Sanitization, such that the PHI cannot be retrieved.

Workforce: Workforce means Hospital's employees, volunteers, trainees, temporary employees, leased employees, and other persons whose conduct, in the performance of work for Hospital, is under the direct control of Hospital, whether or not they are paid by Hospital.

Policy Statements:

1. Breach: Except for the exclusions from the definition of "breach" above, an acquisition, access, use, or disclosure of PHI in a manner not permitted by the HIPAA Rules is presumed to be a breach unless Hospital (or their business associates, if applicable), demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

    A. The nature and extend of the PHI involved, including the types of identifiers and the likelihood of re-identification;

B. The unauthorized person who used the PHI or to whom the disclosure was made;
C. Whether the PHI was actually acquired or viewed; and
D. The extent to which the risk to the PHI has been mitigated.

2. Discovery of Breach: A breach is considered "discovered" on the first day when the incident becomes known to any member of Hospital's workforce. (See attachment for examples of breach of unsecured protected health information.)

   Following the discovery of a potential breach, Hospital shall promptly:

   - Begin an investigation
   - Conduct a risk assessment
   - Determine what required notifications, if any, must be made based on the results of the risk assessment
   - Begin the process to notify each individual whose PHI has been, or is reasonably believed by Hospital to have been, accessed, acquired, used, or disclosed as a result of the breach.
   - Make the necessary external notifications (e.g., Secretary of Department of Health & Human Services, media outlets, law enforcement officials).

3. Breach Investigation: The Privacy Officer or another employee appointed by senior management shall act as the investigator of the breach. The investigator shall be responsible for the management of the breach investigation, completion of a risk assessment, and coordinating with others in Hospital (e.g., administration, human resources, risk management, public relations, and legal counsel). The investigator shall be the key facilitator for all breach notification processes to the appropriate entities (e.g. HHS, media, and law enforcement officials). All documentation related to the breach investigation, including the risk assessment, shall be retained for a minimum of six years.

4. Risk Assessment: To determine if an impermissible use or disclosure of PHI constitutes a reportable breach and requires further notification to individuals, media, or HHS, Hospital, in conjunction with the Privacy Officer, will perform a risk assessment. As provided in Section 1, an unauthorized acquisition, access, use of or disclosure is presumed to be a breach unless the Risk Assessment demonstrates that there is a low probability that the PHI has been compromised. The Privacy Officer shall document the risk assessment as part of the investigation in writing.

   Based on the outcome of the risk assessment, Hospital will determine the need to move forward with breach notification. The risk assessment and the supporting documentation shall be fact specific and address:

   A. Consideration of who impermissibly used or to whom the information was impermissibly disclosed.
   B. Consideration of whether the information was actually accessed or acquired.
   C. The type and amount of PHI involved. If the PHI included name and date of birth, or name and social security number, the government considers such a breach to be reportable.
   D. The potential for risk of financial, reputational, or other harm. Consider whether the patient is at risk for identity theft. Consider the risk to an individual if the information includes potentially embarrassing or sensitive information.
   E. The steps taken to immediately or promptly mitigate any potential consequences of the breach.
   F. Any other information relevant to the assessment of risk.

5. Timeliness of Notifications: Upon determination that breach notification is required, the Privacy Officer shall make arrangements to provide the required notices to the individual(s), media, and HHS, as applicable, in a timely manner, without unreasonable delay and in no case later than 60 calendar days after the discovery of the breach by Hospital or their business associates. It is the responsibility of Hospital to demonstrate in writing that all notifications were made as required, including evidence demonstrating the necessity of delay.

6. Establish a Toll-Free Number for Patients. HIPAA requires that Hospital provide a toll-free number for patients affected by a breach to call to inquire further.

7. Delay of Notification Authorized for Law Enforcement Purposes: If a law enforcement official notifies Hospital that a notification, notice, or posting would impede a criminal investigation or cause damage to national security, Hospital, as applicable, shall temporarily delay breach notification.

   A. If the statement from the law enforcement official is in writing and specifies the time for which a delay is required, delay such notification, notice or posting for the time period specified by the official; or
   B. If the statement is made orally, document the statement in writing, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described above is submitted during that time.

8. Content of the Notice to Individuals: If Hospital determines that a breach occurred, Hospital, as applicable, will prepare a notice to the affected individuals. Other notices may be required as set forth in this policy. If contact information of individuals is not current, substitute notice in the form of a website or newspaper notice may be permissible as provided below.

   The notice to individuals shall be written in plain language, easy to understand, and must contain the following information:

   A. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.
   B. A description of the types of unsecured PHI that were involved in the breach (such as whether full name, Social Security number, date of birth, home address, account number, diagnosis, drugs prescribed, or other types of information were involved).
   C. Any steps the individual should take to protect themselves from potential harm resulting from the breach.
   D. A brief description of what Hospital is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches.
   E. Contact procedures for individuals to ask questions or learn additional information, which includes a toll-free telephone number, an e-mail address, website, or postal address.

9. Notice to Media: Notice shall be provided to prominent media outlets serving the state and regional area *when the breach of unsecured PHI affects more than 500 patients who are residents of Oklahoma (or more than 500 patients in any one state).* The Notice shall be provided in the form of a press release, and contain substantially the same information as the Notice to Individuals in Section 8. Any notice to the media shall be reviewed and approved by legal counsel.

10. Notice to Secretary of HHS: Notice shall be provided to the Secretary of HHS as follows:

    A. For breaches involving 500 or more individuals, Hospital, as applicable, shall notify the Secretary of HHS at the same time notice is made to the individuals. Notice shall be made at the following website: www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html

    B. For breaches involving less than 500 individuals, Hospital, as applicable, will maintain a log of the breaches and annually submit the log to the Secretary of HHS during the year involved (logged breaches occurring during the preceding calendar year to be submitted no later than 60 days after the end of the calendar year).

       Instructions for submitting the log are provided at:
       www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brinstruction.html.

11. Methods of Notification to Individuals: The method of notification will depend on the individuals to be notified. The following methods must be utilized accordingly:

    A. *Written notification by first-class mail to the individual at the last known address of the individual* or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification shall be provided in one or more mailings as information is available. If Hospital knows that the individual is deceased and has the address of the next of kin or personal representative of the individual, written notification by first-class mail to the next of kin or person representative shall be carried out.

B. *Substitute Notice*. In the case where there is insufficient or out-of-date contact information (including a phone number, email address, etc.) that precludes direct written or electronic notification, a substitute form of notice reasonably calculated to reach the individual shall be provided. A substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative.
    1. In a case in which there is insufficient or out-of-date contact information for less than 10 individuals, every reasonable effort will be made to contact the individuals through alternative methods, such as on-line services.
    2. In the case in which there is insufficient or out-of-date contact information for 10 or more individuals, then the substitute notice shall be in the form of either a conspicuous posting for a period of 90 days on the home page of Hospital's website, as applicable, or a conspicuous notice in a major print or broadcast media in Hospital's geographic areas where the individuals affected by the breach likely reside. The notice shall include a toll-free number that remains active for at least 90 days where an individual can learn whether his or her PHI may be included in the breach.

C. *If Hospital determines that notification requires urgency because of possible imminent misuse of unsecured PHI*, notification may be provided by telephone or other means, as appropriate, in addition to the methods noted above.

12. Maintenance of Breach Information Documentation: Hospital shall maintain documentation of all breaches of unsecured PHI regardless of the number of individuals affected. The following information should be documented for each breach:

    A. A description of what happened, including the date of the breach, the date of the discovery of the breach, and the number of patients affected, if known.
    B. A description of the types of unsecured protected health information that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number, etc.).
    C. Whether protected health information was actually viewed or accessed.
    D. The individual or party who reviewed or accessed the information.
    E. A description of the action taken with regard to notification of patients regarding breach.
    F. Resolution steps taken to mitigate the breach and prevent future occurrences.

13. Breach Notification Log: Each of Hospital shall maintain a breach notification log. An example is provided in Attachment C.

14. Business Associate Responsibilities: A business associate ("BA") of Hospital that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured protected health information shall, immediately notify Hospital, as applicable, of such breach. Such notice shall include the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the BA to have been, accessed, acquired, or disclosed during such breach. The BA shall provide Hospital with any other available information that Hospital, as applicable, is required to include in notification to the individual at the time of the notification or promptly thereafter as information becomes available. Upon notification by the BA of discovery of a breach, Hospital will be responsible for notifying affected individuals, media and Secretary of HHS, and documenting the notification. Hospital may terminate the BA agreement if it determines that the BA acted negligently or did not comply with its obligations under its business associate agreement.

15. Workforce Training: Hospital shall train all members of its workforce on the policies and procedures with respect to PHI as necessary and appropriate for the members to carry out their job responsibilities. Workforce members shall also be trained as to how to identify and report breaches within Hospital, as applicable.

16. Complaints: Each of Hospital shall provide a process for individuals to make complaints concerning such entity's patient privacy policies and procedures or its compliance with such policies and procedures. Individuals have the right to complain about Hospital's breach notification process.

17. Sanctions: Each of Hospital shall have in place and apply appropriate sanctions against members of its workforce who fail to comply with privacy policies and procedures.

18. Retaliation/Waiver: Hospital may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the exercise by the individual of any privacy right. Hospital may not require individuals to waive their privacy rights under as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

19. Documentation. Each of Hospital shall maintain all documentation concerning a breach for at least 6 years from the date that the breach occurred.

20. Examples of Potential Breaches (for use in training):

- Employees who do not have a need to know access the electronic health records of a celebrity who is a patient.
- Stolen or lost laptop containing unsecured (not encrypted) protected health information.
- Papers containing protected health information found scattered along roadside after improper storage in truck by business associate responsible for disposal (shredding).
- Posting of patient's health information on Facebook.
- Misdirected e-mail of listing of drug seeking patients to an external group list.
- Lost flash drive containing database of patients that is not encrypted.
- EOB (Explanation of Benefits) sent to wrong guarantor and not retrieved promptly.
- A member of the workforce accessing the health record of divorced spouse for information to be used in a custody hearing without spouse's authorization.
- A workforce member accessing electronic health records for information on friends or family members out of curiosity and without a business-related purpose.
- Employee takes a cell phone picture of patient and transmits photo to friends.
- Hospital records, lab results, or prescriptions given to the wrong patient or a family member who is not authorized to receive them
- Misdirected fax of patient records and not promptly discarded by the receiving party.
- Mobile device with patient-identifying photos lost, and the mobile device is not encrypted.

Sample Notification Letter to Patients – Document to be reviewed and customized prior to use
[Hospital's stationery]

[Date]

[Name here]
[Address here]
[City, State Zip Code]

Dear [Name of Individual]:

I am writing to you with important information about a recent incident involving your personal health information. We became aware of this incident on [Insert Date], which occurred on or about [Insert Date]. The incident occurred as follows:

Describe event and include the following information:

A. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.
B. A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, Social Security number, date of birth, home address, account number, diagnosis, disability code or other types of information were involved).
C. Any steps the individual should take to protect themselves from potential harm resulting from the breach.
D. A brief description of what Hospital, as applicable, is doing to investigate the breach, to mitigate harm to individuals and to protect against further breaches.
E. Contact procedures for individuals to ask questions or learn additional information, which includes a toll-free telephone number, an e-mail address, website, or postal address.

Other optional considerations:
To help ensure that this information is not used inappropriately, [HOSPITAL] will cover the cost for one year for you to receive credit monitoring. To take advantage of this offer, [document how the process would work].

We also advise you to immediately take the following steps:

- Call the toll-free numbers of anyone of the three major credit bureaus (below) to place a fraud alert on your credit report. This can help prevent an identity thief from opening additional accounts in your name. As soon as the credit bureau confirms your fraud alert, the other two credit bureaus will automatically be notified to place alerts on your credit report and all three reports will be sent to you free of charge.

  Equifax: 1-800-525-6285; www.equifax.com; P.O. Box 740241, Atlanta, GA 30374-0241
  Experian: 1-888-EXPERIAN (397-3742); www.experian.com; P.O. Box 9532, Allen, TX 75013
  TransUnion: 1-800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

- Order your credit reports. By establishing a fraud alert, you will receive a follow-up letter that will explain how you can receive a free copy of your credit report. When you receive your credit report, examine it closely, and look for signs of fraud, such as credit accounts that are not yours.

- Continue to monitor your credit reports. Even though a fraud alert has been placed on your account, you should continue to monitor your credit reports to ensure an imposter has not opened an account with your personal information.

We take very seriously our role of safeguarding your personal information and using it in an appropriate manner. We apologize for the stress and worry this situation may have caused you and we are doing everything we can to remedy the situation.

We have established a toll-free number to call us with questions and concerns about the loss of your personal information. You may call [insert toll-free number] during normal business hours with any questions you have.

We have also established a section on our website with updated information and links to websites that offer information on what to do if your personal information has been compromised.

[Insert closing paragraph based upon situation]

Sincerely,

Name
Title

Sample Media Notification Statement/Release if breach involves more than 500 residents of a State – Document to be Reviewed and Customized Prior to Use and Reviewed by Legal Counsel
[Insert Date]
Contact: [Insert Contact Information Including Phone Number/e-mail address]

IMMEDIATE RELEASE

HOSPITAL NOTIFIES PATIENTS OF BREACH OF UNSECURED PERSONAL INFORMATION

[HOSPITAL] notified [insert number] patients of a breach of unsecured personal patient protected health information after discovering the following event:

Describe event and include the following information as communicated to the victims:

A. A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.
B. A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, Social Security number, date of birth, home address, account number, diagnosis, disability code or other types of information were involved).
C. Any steps the individual should take to protect themselves from potential harm resulting from the breach.
D. A brief description of what Hospital, as applicable, is doing to investigate the breach, to mitigate harm to individuals and to protect against further breaches.
E. Contact procedures for individuals to ask questions or learn additional information, which includes a toll-free telephone number, an e-mail address, website, or postal address.

In conjunction with local law enforcement and security experts, [HOSPITAL] is working to notify impacted patients to mitigate the damages of the breach. [HOSPITAL] has in place safeguards to ensure the privacy and security of all patient health information. As a result of this breach, steps are underway to further improve the security of its operations and eliminate future risk. In a notification to patients, [HOSPITAL] has offered their resources as well as [insert as applicable]. [HOSPITAL] also has encouraged its patients to contact their financial institutions to prevent unauthorized access to personal accounts.

[HOSPITAL] has trained staff available for you to call with any questions related to the data breach. Patients may call [insert phone number here] from [insert hours] with any questions. In addition, patients may visit [HOSPITAL'S] website at [insert web address] for further information.

"[HOSPITAL] understands the importance of safeguarding our patients' personal information and takes that responsibility very seriously," said [insert name], President. "We will do all we can to work with our patients whose personal information may have been compromised and help them work through the process. We regret that this incident has occurred, and we are committed to prevent future such occurrences. We appreciate the support of our patients during this time."

Please direct all questions to [enter contact information].

Attachment C

Breach Notification Log

Tracking Number	Date of Discovery	Date of Breach	Location	Brief Description of Breach	Number of Patients Involved	Notification Dates			Actions Taken/ Resolution Steps
						Patients	HHS	Media	

COMPLAINT ABOUT USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION

We are a health care provider and a "covered entity" subject to state and federal laws that require us to protect the privacy of the health information we maintain about our patients. We call this law the "Privacy Rule". We must provide a process for you to complain about our health information policies and procedures or non-compliance with them or the Privacy Rule. We will not retaliate against anyone who files a complaint about us in good faith.

Claimant Information

Your Name:_____
(Please print)

Your Address:_____

Your Telephone Number:_____

Your Email Address:_____

What is the best way to reach you?_____

What is the best time to reach you?_____

I wish to file a privacy complaint against Community Hospital, LLC or TPG Hospital, LLC d/b/a Northwest Surgical Hospital (as applicable, the "Hospital"), as described below.

Details of Your Complaint

Whose health information privacy rights were violated (yours or someone else's)?

First Name:_____ Last Name:_____
(Please print) ***(Please print)***

Who at the Hospital (or on behalf of the Hospital) do you believe violated your (or someone else's) health information privacy rights or committed another violation of the Privacy Rule?

Person(s) /Organization(s):
_____
_____
_____

(Please print)

When do you believe the violation of health information privacy rights occurred?

Date(s):_____
_____
_____

(Please print)

Describe what happened. How and why do you believe your (or someone else's) health information privacy rights were violated, or the Privacy Rule otherwise was violated? Please be as specific as possible. Please attach additional sheets of paper as needed.

_____
_____
_____
_____
_____
_____
_____
_____
_____

(Please print)

Information on how and where to file your complaint are on the last page of this form.

By signing this complaint form, you acknowledge and agree that, unless we are prohibited from doing so by law, we may use and disclose the information you provided to us in order to conduct an investigation of your allegations and to take such actions as are necessary or desirable for us to address any issues of non-compliance with our health information policies and procedures and the Privacy Rule.

Your Signature :_____ Date:_____

How and Where to File Your Complaint

You may file your written complaint with the Hospital, by mail, fax, or e-mail, by submitting this completed form to the Hospital's Privacy Officer.

If you have any questions regarding how to file a complaint with the Hospital, please contact the Hospital's Privacy Officer.

You may also file a written complaint with the U.S. Department of Health and Human Services, Office for Civil Rights ("OCR"). You must file your complaint with the OCR within 180 days of when you knew or should have known that the act or omission complained of occurred. The OCR may extend the 180-day period if you can show "good cause." The OCR recommends that you use the OCR ***Health Information Privacy Complaint Form Package*** to file a complaint with them. This package, together with other helpful information on how to file a complaint with the OCR, is available on the OCR website at http://www.hhs.gov/ocr/privacy/hipaa/complaints/. You may file a written complaint with the OCR, either on paper or electronically, by mail, fax, or e-mail. To submit a complaint to the OCR by mail or fax, you must submit it to the regional office where the alleged violation took place. The OCR regional office for our Hospital is Region IV and the contact information is as follows:

Office for Civil Rights, DHHS
61 Forsyth Street, SW. – Suite 3B70
Atlanta, GE 30303-8909
(T:) 404-562-7886
(TDD:)404-331-2867
(F:) 404-562-7881

To submit an electronic complaint with the OCR, go to the OCR's website at:
http://www.hhs.gov/ocr/privacyhowtofile.html.

BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement (the "Agreement") is made and entered into this ___ day of _____, 20___ (the "Effective Date"), by and between Community Hospital, LLC ("Covered Entity") and _____ ("Business Associate"). This Agreement supersedes all other agreements, written or oral, between the parties as to the subject matter hereof.

Recitals

A. The purpose of this Agreement is to comply with the "business associate" requirements of the privacy rule and security rule promulgated by the United States Department of Health and Human Services ("DHHS") pursuant to the Health Insurance Portability and Accountability Act of 1996, as it may be amended from time to time, including the amendments promulgated under the Health Information Technology for Economic & Clinical Health Act (collectively, the "Privacy Rule").

B. Business Associate provides services for or on behalf of Covered Entity pursuant to a service agreement or other vendor arrangement ("Service Agreement") that involves the use, disclosure, and/or creation of certain Protected Health Information ("PHI").

The parties desire to enter into this Agreement to prescribe the manner in which Covered Entity's PHI will be handled by Business Associate.

NOW, THEREFORE, in consideration of the foregoing and of the mutual covenants and agreements hereinafter addressed, the parties agree as follows:

1. Definitions. Capitalized terms used in this Agreement shall have the meaning ascribed to them in this Agreement and in the Privacy Rule.

2. Responsibilities of Business Associate. With regard to the use and disclosure of PHI, Business Associate hereby agrees as follows:

a. Use and Disclosure of PHI. Business Associate shall use PHI only as permitted or required by applicable law, the terms of this Agreement, or the Service Agreement, provided that in any case, such use or disclosure would not constitute a violation of the Privacy Rule if done by Covered Entity. Notwithstanding the foregoing, Business Associate may:

(i) Use PHI and disclose PHI to its employees, in either case for management, administration, or other purposes deemed necessary to carry out Business Associate's responsibilities under this Agreement and the Service Agreement, provided that Business Associate may disclose PHI to its employees only if Business Associate (A) advises the employees of Business Associate's obligations under this Agreement and of the consequences to the employees and Business Associate for violating such obligations, and (B) takes appropriate disciplinary action against any employee who uses or discloses PHI in violation of this Agreement;

(ii) Disclose PHI to a third party for management and administration purposes as necessary to carry out Business Associate's responsibilities under this Agreement and the Service Agreement, if (A) the disclosure is required by law, or (B) Business Associate obtains reasonable assurances from the recipient of the PHI that (1) the PHI will remain confidential and will be used or further disclosed only as required by law or for the purpose for which it was disclosed to the recipient; (2) that the recipient will notify Business Associate of any breach of confidentiality of PHI; and (3) the recipient agrees to be bound by the same restrictions on the use and disclosure of PHI that apply to Business Associate under this Agreement;

(iii) Upon the request of Covered Entity, provide data aggregation services related to the healthcare operations of Covered Entity in accordance with the provisions of the Privacy Rule.

(iv) In each instance that Business Associate engages any person other than a member of Business Associate's workforce and delegates to that person any part of the services to be performed on behalf of the Covered Entity (a "Subcontractor"), Business Associate shall enter in a written agreement with the Subcontractor requiring Subcontractor to (a) appropriately safeguard PHI created, received, maintained, or transmitted on behalf of Business Associate; and (b) comply with the same restrictions and conditions imposed under this Agreement upon Business Associate Taft with respect to PHI.

b. Safeguards. Business Associate shall comply with the applicable requirements of Subpart C of 45 C.F.R. Part 164 regarding security of electronic PHI. Business Associate shall (i) use all appropriate safeguards to prevent any use or disclosure of PHI other than as permitted by the terms of this Agreement, (ii) provide Covered Entity with any requested information regarding such safeguards, and (iii) give Covered Entity access to Business Associate's facilities used for the maintenance or processing of PHI and to its books, practices, records, policies, and procedures concerning the use and disclosure of PHI for the purpose of determining Business Associate's compliance with this Agreement. If PHI is transmitted, maintained, or received electronically ("Electronic PHI"), Business Associate shall use administrative, technical, and physical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of Electronic PHI, including access controls, workstation security, integrity controls, data backup and storage, and encryption, except as otherwise permitted by this Agreement. Business Associate shall develop and maintain HIPAA policies and procedures and conduct HIPAA training applicable to all any employees and others performing services on behalf of Business Associate that will perform services under this Agreement.

(i) Reporting. Business Associate shall report to the Privacy Officer of Covered Entity as soon as possible but in no event later than 30 days after Business Associate becomes aware of any (A) use, disclosure, access, or acquisition of PHI not permitted under the terms of this Agreement, or (B) any security incident involving Electronic PHI (either, a "Potential Breach"). Business Associate shall fully cooperate with Covered Entity and assist Covered Entity in investigating the Potential Breach. Business Associate shall provide the following information to Covered Entity within the 30-day period: (A) a brief description of the Potential Breach; (B) a description of the types of PHI involved in the Potential Breach; (C)

steps that an individual may take to protect themselves from potential harm resulting from the Potential Breach; (D) a description of Business Associate's actions to mitigate the consequences of the Potential Beach and to prevent further incidents; and (E) if requested by Covered Entity, contact procedures for individuals to contact Business Associate for additional information. Covered Entity shall make the final determination regarding whether the Potential Breach is reportable to any individual, DHHS, or the media, and shall be responsible for reporting if applicable. Both parties shall keep any Potential Breach and the investigation strictly confidential.

(ii) Mitigation. Business Associate shall, to the extent practicable, mitigate any harmful effect known to Business Associate resulting from a use or disclosure of PHI by Business Associate, its agents, or subcontractors in violation of this Agreement.

(iii) Access to PHI by Patients. To enable Covered Entity to comply with a patient's request to access the patient's PHI maintained in a Designated Record Set, Business Associate shall make requested PHI available to Covered Entity within five (5) days of receiving a request for access from Covered Entity.

(iv) Amendment of PHI. To enable Covered Entity to respond to a patient's request for amendment of the patient's PHI maintained in a Designated Record Set, Business Associate shall make the requested PHI available to Covered Entity within ten (10) days of receiving a request from Covered Entity and incorporate any such amendments in the patient's PHI in accordance with the Privacy Rule requirements.

(v) Accounting of Disclosures. To enable Covered Entity to respond to a patient's request for accounting of disclosures of the patient's PHI, Business Associate shall (A) document all disclosures of PHI by Business Associate, and (B) within ten (10) days of receiving a request for accounting from Covered Entity, make available to Covered Entity the following information concerning disclosures of the patient's PHI by Business Associate: the date of disclosure, the name and address, if known, of the recipient of the patient's PHI, a brief description of the patient's PHI disclosed, and a brief statement of the purpose of the disclosure.

(vi) Disclosures to Secretary of DHHS. Business Associate shall make all internal practices, books, and records relating to the use and disclosure of PHI received or created by Business Associate on behalf of Covered Entity available to the Secretary of DHHS for the purpose of determining Covered Entity's compliance with the Privacy Rule.

3. Responsibilities of Covered Entity. With regard to the use and/or disclosure of PHI by Business Associate, Covered Entity hereby agrees as follows:

a. Covered Entity shall provide Business Associate with a copy of Covered Entity's notice of privacy practices promptly following execution of this Agreement and upon any change to such notice;

b. Covered Entity shall inform Business Associate of any changes in, or revocation of, an authorization provided to Covered Entity by a patient to the extent that such change or revocation would impact Business Associate's right to use and/or disclose PHI pursuant to this Agreement; and

c. Covered Entity shall timely notify Business Associate, in writing, of any restrictions on the use and/or disclosure of PHI to which Covered Entity has agreed in accordance with the Privacy Rule to the extent that such restriction would impact Business Associate's right to use and/or disclose PHI pursuant to this Agreement.

4. Term and Termination.

a. Term. Unless earlier terminated pursuant to Section 4(b) below, this Agreement shall become effective on the Effective Date and shall continue in effect until the later to occur of (i) the termination of the Service Agreement, or (ii) the discontinuation of Business Associate's provision of services to Covered Entity involving the use, disclosure, and/or creation of PHI. This Agreement replaces and supersedes any previous HIPAA business associate agreement between the parties with respect to the Service Agreement.

b. Termination. Notwithstanding Section 4(a) above, this Agreement may be terminated as follows:

(i) Upon mutual written agreement of the parties; or

(ii) If Covered Entity determines that Business Associate breached any provision of this Agreement, Covered Entity shall have the right to either (A) immediately terminate this Agreement without providing Business Associate an opportunity to cure the breach, or (B) provide Business Associate with a written notice of breach and terminate the Agreement if Business Associate does not cure the breach within thirty (30) days of receiving such notice.

c. Effect of Termination. Upon termination of this Agreement, Business Associate shall return to Covered Entity or destroy, as requested by Covered Entity, PHI in Business Associate's possession and retain no copies or back-up records of the PHI. If such return or destruction is infeasible, as determined by the parties, the obligations set forth in this Agreement with respect to the PHI shall survive termination and Business Associate shall limit any further use and disclosure of PHI to the purposes that make the return or destruction of PHI infeasible.

5. Indemnification. Business Associate agrees to indemnify and hold harmless Covered Entity and its affiliates, directors, officers, employees, and agents (individually and collectively, "Covered Entity Indemnitee") against any and all losses, liabilities, judgments, penalties, awards, and costs (including costs related to reporting breaches to any individuals, the government, and the media, and establishing a toll-free phone line as required by the Privacy Rule; investigation; and legal fees and expenses) arising out of or related to (a) a breach of this Agreement by Business Associate, or (b) any negligent or wrongful acts or omissions of Business Associate or its employees, directors, officers, subcontractors, or agents, including failure to perform their obligations under the Privacy Rule.

6. **Amendment**. This Agreement may be modified or amended only upon mutual written consent of the parties. The parties agree to take any action required to amend this Agreement if Covered Entity, in its reasonable discretion, determines that an amendment is necessary for Covered Entity to comply with the requirements of the Privacy Rule or any other law or regulation affecting the use or disclosure of PHI.

7. **Assignment**. Business Associate may not assign its rights and obligations under this Agreement without the prior written consent of Covered Entity; Covered Entity may assign its rights and obligations under this Agreement upon providing prior written notice of assignment to Business Associate.

8. **Notices**. Any notices to be given hereunder shall be deemed effectively given when personally delivered, received by electronic means (including facsimile) or overnight courier, or five (5) calendar days after being deposited in the United States mail, with postage prepaid thereon, certified or registered mail, return receipt requested, addressed as follows:

If to Business Associate: _____

_____

_____

If to Covered Entity: Privacy Officer
Community Hospital, LLC
14024 Quail Pointe Drive
Oklahoma City, OK 73134

9. **Independent Contractor.** Business Associate is performing services for Covered Entity as an independent contractor. Nothing in this Agreement shall be construed as creating an agency, partnership, employment, or joint venture relationship between Covered Entity and Business Associate. Business Associate may not bind, or create any obligations on behalf of, Covered Entity.

10. **Survival**. The obligations of Business Associate under the provisions of Sections 2(b) (with respect to PHI retained by Business Associate following termination of this Agreement), 4(c), and 5 shall survive the termination of this Agreement indefinitely.

11. **No Third Party Beneficiaries**. Nothing expressed or implied in this Agreement is intended to confer, nor anything herein shall confer, upon any person other than the parties hereto any rights, remedies, obligations, or liabilities whatsoever.

12. **Waiver**. A waiver by either party of a breach or failure to perform hereunder shall not constitute a waiver of any subsequent breach or failure.

13. **Counterparts**. This Agreement may be executed in counterparts, each of which shall be deemed to be an original and all of which together shall constitute one and the same instrument.

14. Governing Law. This Agreement shall be governed by, construed, interpreted, and enforced under the laws of the state of Oklahoma.

IN WITNESS WHEREOF, each of the undersigned has caused this Agreement to be duly executed in its name and on its behalf effective as of the Effective Date.

BUSINESS ASSOCIATE	**COVERED ENTITY**
By:_____	By:_____
Name:_____	Name: _____
Title:_____	Title:_____

BUSINESS ASSOCIATE AGREEMENT

This Business Associate Agreement (the "Agreement") is made and entered into this ___ day of _____, 20___ (the "Effective Date"), by and between TPG Hospital, LLC d/b/a Northwest Surgical Hospital ("Covered Entity") and _____ ("Business Associate"). This Agreement supersedes all other agreements, written or oral, between the parties as to the subject matter hereof.

Recitals

A. The purpose of this Agreement is to comply with the "business associate" requirements of the privacy rule and security rule promulgated by the United States Department of Health and Human Services ("DHHS") pursuant to the Health Insurance Portability and Accountability Act of 1996, as it may be amended from time to time, including the amendments promulgated under the Health Information Technology for Economic & Clinical Health Act (collectively, the "Privacy Rule").

B. Business Associate provides services for or on behalf of Covered Entity pursuant to a service agreement or other vendor arrangement ("Service Agreement") that involves the use, disclosure, and/or creation of certain Protected Health Information ("PHI").

The parties desire to enter into this Agreement to prescribe the manner in which Covered Entity's PHI will be handled by Business Associate.

NOW, THEREFORE, in consideration of the foregoing and of the mutual covenants and agreements hereinafter addressed, the parties agree as follows:

1. Definitions. Capitalized terms used in this Agreement shall have the meaning ascribed to them in this Agreement and in the Privacy Rule.

2. Responsibilities of Business Associate. With regard to the use and disclosure of PHI, Business Associate hereby agrees as follows:

a. Use and Disclosure of PHI. Business Associate shall use PHI only as permitted or required by applicable law, the terms of this Agreement, or the Service Agreement, provided that in any case, such use or disclosure would not constitute a violation of the Privacy Rule if done by Covered Entity. Notwithstanding the foregoing, Business Associate may:

(i) Use PHI and disclose PHI to its employees, in either case for management, administration, or other purposes deemed necessary to carry out Business Associate's responsibilities under this Agreement and the Service Agreement, provided that Business Associate may disclose PHI to its employees only if Business Associate (A) advises the employees of Business Associate's obligations under this Agreement and of the consequences to the employees and Business Associate for violating such obligations, and (B) takes appropriate disciplinary action against any employee who uses or discloses PHI in violation of this Agreement;

(ii) Disclose PHI to a third party for management and administration purposes as necessary to carry out Business Associate's responsibilities under this Agreement and the Service Agreement, if (A) the disclosure is required by law, or (B) Business Associate obtains reasonable assurances from the recipient of the PHI that (1) the PHI will remain confidential and will be used or further disclosed only as required by law or for the purpose for which it was disclosed to the recipient; (2) that the recipient will notify Business Associate of any breach of confidentiality of PHI; and (3) the recipient agrees to be bound by the same restrictions on the use and disclosure of PHI that apply to Business Associate under this Agreement;

(iii) Upon the request of Covered Entity, provide data aggregation services related to the healthcare operations of Covered Entity in accordance with the provisions of the Privacy Rule.

(iv) In each instance that Business Associate engages any person other than a member of Business Associate's workforce and delegates to that person any part of the services to be performed on behalf of the Covered Entity (a "Subcontractor"), Business Associate shall enter in a written agreement with the Subcontractor requiring Subcontractor to (a) appropriately safeguard PHI created, received, maintained, or transmitted on behalf of Business Associate; and (b) comply with the same restrictions and conditions imposed under this Agreement upon Business Associate Taft with respect to PHI.

b. Safeguards. Business Associate shall comply with the applicable requirements of Subpart C of 45 C.F.R. Part 164 regarding security of electronic PHI. Business Associate shall (i) use all appropriate safeguards to prevent any use or disclosure of PHI other than as permitted by the terms of this Agreement, (ii) provide Covered Entity with any requested information regarding such safeguards, and (iii) give Covered Entity access to Business Associate's facilities used for the maintenance or processing of PHI and to its books, practices, records, policies, and procedures concerning the use and disclosure of PHI for the purpose of determining Business Associate's compliance with this Agreement. If PHI is transmitted, maintained, or received electronically ("Electronic PHI"), Business Associate shall use administrative, technical, and physical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of Electronic PHI, including access controls, workstation security, integrity controls, data backup and storage, and encryption, except as otherwise permitted by this Agreement. Business Associate shall develop and maintain HIPAA policies and procedures and conduct HIPAA training applicable to all any employees and others performing services on behalf of Business Associate that will perform services under this Agreement.

(i) Reporting. Business Associate shall report to the Privacy Officer of Covered Entity as soon as possible but in no event later than 30 days after Business Associate becomes aware of any (A) use, disclosure, access, or acquisition of PHI not permitted under the terms of this Agreement, or (B) any security incident involving Electronic PHI (either, a "Potential Breach"). Business Associate shall fully cooperate with Covered Entity and assist Covered Entity in investigating the Potential Breach. Business Associate shall provide the following information to Covered Entity within the 30-day period: (A) a brief description of the Potential Breach; (B) a description of the types of PHI involved in the Potential Breach; (C)

steps that an individual may take to protect themselves from potential harm resulting from the Potential Breach; (D) a description of Business Associate's actions to mitigate the consequences of the Potential Beach and to prevent further incidents; and (E) if requested by Covered Entity, contact procedures for individuals to contact Business Associate for additional information. Covered Entity shall make the final determination regarding whether the Potential Breach is reportable to any individual, DHHS, or the media, and shall be responsible for reporting if applicable. Both parties shall keep any Potential Breach and the investigation strictly confidential.

(ii) Mitigation. Business Associate shall, to the extent practicable, mitigate any harmful effect known to Business Associate resulting from a use or disclosure of PHI by Business Associate, its agents, or subcontractors in violation of this Agreement.

(iii) Access to PHI by Patients. To enable Covered Entity to comply with a patient's request to access the patient's PHI maintained in a Designated Record Set, Business Associate shall make requested PHI available to Covered Entity within five (5) days of receiving a request for access from Covered Entity.

(iv) Amendment of PHI. To enable Covered Entity to respond to a patient's request for amendment of the patient's PHI maintained in a Designated Record Set, Business Associate shall make the requested PHI available to Covered Entity within ten (10) days of receiving a request from Covered Entity and incorporate any such amendments in the patient's PHI in accordance with the Privacy Rule requirements.

(v) Accounting of Disclosures. To enable Covered Entity to respond to a patient's request for accounting of disclosures of the patient's PHI, Business Associate shall (A) document all disclosures of PHI by Business Associate, and (B) within ten (10) days of receiving a request for accounting from Covered Entity, make available to Covered Entity the following information concerning disclosures of the patient's PHI by Business Associate: the date of disclosure, the name and address, if known, of the recipient of the patient's PHI, a brief description of the patient's PHI disclosed, and a brief statement of the purpose of the disclosure.

(vi) Disclosures to Secretary of DHHS. Business Associate shall make all internal practices, books, and records relating to the use and disclosure of PHI received or created by Business Associate on behalf of Covered Entity available to the Secretary of DHHS for the purpose of determining Covered Entity's compliance with the Privacy Rule.

3. Responsibilities of Covered Entity. With regard to the use and/or disclosure of PHI by Business Associate, Covered Entity hereby agrees as follows:

a. Covered Entity shall provide Business Associate with a copy of Covered Entity's notice of privacy practices promptly following execution of this Agreement and upon any change to such notice;

b. Covered Entity shall inform Business Associate of any changes in, or revocation of, an authorization provided to Covered Entity by a patient to the extent that such change or revocation would impact Business Associate's right to use and/or disclose PHI pursuant to this Agreement; and

c. Covered Entity shall timely notify Business Associate, in writing, of any restrictions on the use and/or disclosure of PHI to which Covered Entity has agreed in accordance with the Privacy Rule to the extent that such restriction would impact Business Associate's right to use and/or disclose PHI pursuant to this Agreement.

4. Term and Termination.

a. Term. Unless earlier terminated pursuant to Section 4(b) below, this Agreement shall become effective on the Effective Date and shall continue in effect until the later to occur of (i) the termination of the Service Agreement, or (ii) the discontinuation of Business Associate's provision of services to Covered Entity involving the use, disclosure, and/or creation of PHI. This Agreement replaces and supersedes any previous HIPAA business associate agreement between the parties with respect to the Service Agreement.

b. Termination. Notwithstanding Section 4(a) above, this Agreement may be terminated as follows:

(i) Upon mutual written agreement of the parties; or

(ii) If Covered Entity determines that Business Associate breached any provision of this Agreement, Covered Entity shall have the right to either (A) immediately terminate this Agreement without providing Business Associate an opportunity to cure the breach, or (B) provide Business Associate with a written notice of breach and terminate the Agreement if Business Associate does not cure the breach within thirty (30) days of receiving such notice.

c. Effect of Termination. Upon termination of this Agreement, Business Associate shall return to Covered Entity or destroy, as requested by Covered Entity, PHI in Business Associate's possession and retain no copies or back-up records of the PHI. If such return or destruction is infeasible, as determined by the parties, the obligations set forth in this Agreement with respect to the PHI shall survive termination and Business Associate shall limit any further use and disclosure of PHI to the purposes that make the return or destruction of PHI infeasible.

5. Indemnification. Business Associate agrees to indemnify and hold harmless Covered Entity and its affiliates, directors, officers, employees, and agents (individually and collectively, "Covered Entity Indemnitee") against any and all losses, liabilities, judgments, penalties, awards, and costs (including costs related to reporting breaches to any individuals, the government, and the media, and establishing a toll-free phone line as required by the Privacy Rule; investigation; and legal fees and expenses) arising out of or related to (a) a breach of this Agreement by Business Associate, or (b) any negligent or wrongful acts or omissions of Business Associate or its employees, directors, officers, subcontractors, or agents, including failure to perform their obligations under the Privacy Rule.

6. **Amendment**. This Agreement may be modified or amended only upon mutual written consent of the parties. The parties agree to take any action required to amend this Agreement if Covered Entity, in its reasonable discretion, determines that an amendment is necessary for Covered Entity to comply with the requirements of the Privacy Rule or any other law or regulation affecting the use or disclosure of PHI.

7. **Assignment**. Business Associate may not assign its rights and obligations under this Agreement without the prior written consent of Covered Entity; Covered Entity may assign its rights and obligations under this Agreement upon providing prior written notice of assignment to Business Associate.

8. **Notices**. Any notices to be given hereunder shall be deemed effectively given when personally delivered, received by electronic means (including facsimile) or overnight courier, or five (5) calendar days after being deposited in the United States mail, with postage prepaid thereon, certified or registered mail, return receipt requested, addressed as follows:

If to Business Associate: _____

_____

_____

If to Covered Entity: Privacy Officer
Healthcare Partners Investments, LLC
14024 Quail Pointe Drive
Oklahoma City, OK 73134

9. **Independent Contractor.** Business Associate is performing services for Covered Entity as an independent contractor. Nothing in this Agreement shall be construed as creating an agency, partnership, employment, or joint venture relationship between Covered Entity and Business Associate. Business Associate may not bind, or create any obligations on behalf of, Covered Entity.

10. **Survival**. The obligations of Business Associate under the provisions of Sections 2(b) (with respect to PHI retained by Business Associate following termination of this Agreement), 4(c), and 5 shall survive the termination of this Agreement indefinitely.

11. **No Third Party Beneficiaries**. Nothing expressed or implied in this Agreement is intended to confer, nor anything herein shall confer, upon any person other than the parties hereto any rights, remedies, obligations, or liabilities whatsoever.

12. **Waiver**. A waiver by either party of a breach or failure to perform hereunder shall not constitute a waiver of any subsequent breach or failure.

13. **Counterparts**. This Agreement may be executed in counterparts, each of which shall be deemed to be an original and all of which together shall constitute one and the same instrument.

14. Governing Law. This Agreement shall be governed by, construed, interpreted, and enforced under the laws of the state of Oklahoma.

IN WITNESS WHEREOF, each of the undersigned has caused this Agreement to be duly executed in its name and on its behalf effective as of the Effective Date.

BUSINESS ASSOCIATE	**COVERED ENTITY**
By:_____	By:_____
Name:_____	Name: _____
Title:_____	Title:_____

Community Hospital &
TPG Hospital, LLC d/b/a Northwest Surgical Hospital
HIPAA Privacy & Security Policies & Procedures
Employee/Associate Pledge for Confidentiality

I, the undersigned, have read and understand Community Hospital & TPG Hospital, LLC d/b/a Northwest Surgical Hospital (collectively referred to herein as the "Hospital") policy on Health Information Privacy Policies and Procedures and HIPAA Security Policy, copies of which are made available on the intranet or by request from the HR department. In consideration of my employment or association with the Hospital, and as an integral part of the terms and conditions of my employment or association, I hereby agree that I will not at any time, during my employment or association or after my employment or association, access or use health information, or reveal or disclose to any persons within or outside the Hospital, any health information except as may be required in the course of my duties and responsibilities and in accordance with applicable law and the Hospital policies governing proper release of information. I also understand that unauthorized use or disclosure of such information will result in disciplinary action up to and including termination of employment or association with the Hospital and the imposition of fines pursuant to applicable state and federal laws.

Signature: _____

Printed Name: _____

Date: _____

Community Hospital, LLC *Effective March 1, 2014*
TPG Hospital, LLC d/b/a Northwest Surgical Hospital

HIPAA SECURITY POLICY

PART I- GENERAL

1. Policy Statement – Affiliated Covered Entities

The respective governing bodies of Community Hospital, LLC and TPG Hospital, LLC d/b/a Northwest Surgical Hospital (collectively, the "Hospitals" and each a "Hospital") have designated the Hospitals as affiliated covered entities for purposes of compliance with the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations ("HIPAA"). Each of the entities are under common ownership or control, as defined in 45 CFR §§ 164.102 and 164.105(b). It is the policy of the Hospitals to safeguard the PHI in accordance with the requirements of HIPAA and the Security Standards for the Protection of Electronic Protected Health Information (45 C.F.R. Parts 160 & 164) (the "Security Rule"). This Policy governs the use and disclosure of electronic PHI by the Hospitals.

2. Definitions

2.1 ***Administrative Safeguards*** are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect ePHI and to manage the conduct of the Hospitals' workforce in relation to the protection of that information.

2.2 ***ePHI*** is protected health information that is transmitted by or maintained in Electronic Media.

2.3 ***Protected Health Information*** (PHI) is the information that is subject to and defined in the Hospitals' privacy policies and procedures.

2.4 ***Electronic Media*** means:

(1) Electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or

(2) Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet (wide-open), extranet (using Internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. *Certain transmissions, including paper, facsimile, and voice via telephone are not considered to be transmissions via Electronic Media, because the information being exchanged did not exist in electronic form before the transmission.*

2.5 ***Personnel*** means employees, volunteers, trainees and other persons whose conduct in the performance of work for the Hospitals is under direct control of the Hospitals, whether or not paid by the Hospitals.

2.6 ***Physical Safeguards*** are physical measures, policies, and procedures to protect the Hospitals' electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.

2.7 ***Security Incident*** means the attempted or unsuccessful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system.

2.8 ***Technical Safeguards*** means the technology and the policy and procedures for its use that protect ePHI and control access to it.

3. Privacy Officer

3.1 Diana Waddell is the Privacy Officer for the Hospitals. The Privacy Officer shall serve as the security official required by the Security Rule and is responsible for the development and implementation of the Hospitals' policies and procedures relating to security of ePHI, including but not limited to this Policy.

4. Disclosures of Electronic PHI to Business Associates

4.1 A business associate, as defined in the HIPAA Privacy Policies and Procedures, may create, receive, maintain, or transmit ePHI on behalf of the applicable Hospital if such Hospital first obtains satisfactory assurances from the business associate that it will appropriately safeguard the information. Such satisfactory assurances shall be documented through a written contract providing that the business associate will:

- Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the ePHI that the business associate creates, receives, maintains, or transmits on behalf of the applicable Hospital (the Contract ePHI);
- Ensure that any agents or subcontractors to whom the business associate provides Contract ePHI agree to implement reasonable and appropriate security measures to protect the Contract ePHI;
- Report to the applicable Hospital any Security Incident of which the business associate becomes aware; and
- Authorize termination of the contract by the applicable Hospital if such Hospital determines that the business associate has violated a material term of the contract.

5. Sanction Policy

5.1 Sanctions are applied against Personnel who fail to comply with the security policies and procedures and practices of the Hospitals.

5.2 All Personnel are required to adhere to this Policy and the security policies and procedures and practices of the Hospitals and are made aware that sanctions will be applied for non-compliance.

5.3 Sanctions for security violations are applied uniformly across all job categories.

5.4 The Privacy Officer in consultation with the administrator of each Hospital, as applicable, determines the necessary and appropriate sanctions based on the type of security violation, its severity and whether it was intention or unintentional.

5.5 Sanctions may include verbal warnings, written warnings, probationary periods, termination of access rights to ePHI, termination of employment and other disciplinary action authorized by the Hospitals' personnel policies.

PART II – ADMINISTRATIVE SAFEGUARDS

6. Workforce Security

6.1 The Hospitals' policies and procedures attempt to ensure that Personnel have appropriate access to ePHI if required for their job duties and prevent Personnel who do not have access from obtaining access to ePHI.

6.2 Personnel who work with ePHI or in areas where it may be accessed have received appropriate authorization to do so.

6.3 Non-employees, including maintenance personnel or software vendors, who work with ePHI or in areas where it may be accessed must receive appropriate authorization from the Privacy Officer and supervision while on-site.

6.4 The hiring practices of the Hospitals include reference and background checks and other appropriate mechanisms to ensure that access to ePHI is appropriate.

6.5 When an employee is no longer employed by (or affiliated with) the Hospitals, access privileges to ePHI are terminated as soon as the ending of employment is effective, or sooner if circumstances warrant.

7. Information Access Management

7.1 Access to ePHI is authorized, established, maintained and modified based on the minimum amount of protected health information necessary for Personnel to perform their jobs effectively.

7.2 Authorization to access ePHI is consistent with the Hospitals' documented determinations of the minimum amount of protected health information needed by an employee to perform his or her job effectively under the Privacy Rule.

7.3 After access privileges have been authorized, a user account is established that enables an employee to access ePHI and the Hospitals' information systems as appropriate to his or her job function.

7.4 Documentation is maintained of all user accounts and authorized access privileges.

7.5 Reviews of access rights and user accounts are conducted at regular intervals to ensure continued appropriateness of accounts and levels of access.

7.6 Access privileges are modified or revoked whenever a user's job function or access requires changes. Modifications to user accounts are made with appropriate authorization.

7.7 Access privileges are revoked when a user is no longer employed by the Hospitals. This revocation occurs on the effective date of the user's end of employment or sooner if warranted by circumstances.

8. Security Awareness and Training

8.1 Periodic security reminders are provided to Personnel to ensure awareness of security issues and concerns related to protected health information.

8.2 Personnel receive security training as appropriate to their job responsibilities and whenever there are changes to the Hospitals' security environment.

8.3 Personnel receive information on the Hospitals' policies and procedures related to protection from malicious software, log-in monitoring, password management and reporting Security Incidents.

9. Password Management

9.1 The Hospitals follow accepted standards of practice for creating, changing and safeguarding passwords.

9.2 Personnel are required to create passwords for user accounts, email and screensaver protection.

9.3 Passwords must contain at least 6 alphanumeric and not be words that are found in a dictionary.

9.4 Passwords should not be based on personal information such as nicknames, family names, birth dates or other information that may be easily guessed.

9.5 Group passwords are not allowed.

9.6 Personnel are required to change all passwords regularly. Previously used passwords may not be reused.

10. Protection From Malicious Software

10.1 The Hospitals have systems and processes in place for guarding against, detecting and reporting malicious software.

10.2 Anti-virus software with current virus definition files is installed on all desktops, laptops and servers and programmed to conduct automatic virus scanning.

10.3 Security patches and updates for computer operating systems and software are installed to reduce known vulnerabilities.

10.4 Members of the workforce are not allowed to download software from the Internet or install software on desktops or laptops without prior authorization.

10.5 Members of the workforce are not allowed to open email attachments from unknown or untrustworthy sources.

10.6 All e-mail attachments from known and trustworthy sources must be scanned for the presence of viruses.

10.7 When the presence of a virus is suspected or detected, the IS Department must be notified as soon as possible.

10.8 Sanctions are applied against Personnel who violate the Hospitals' protection from malicious software procedures and practices.

11. Security Incidents

11.1 Personnel are trained to report suspected or actual Security Incidents to the Privacy Officer as soon as practicable.

11.2 Security Incidents are documented on the Security Incident Response Report Form. (Exhibit A)

11.3 The Privacy Officer conducts an investigation of all Security Incidents.

11.4 An appropriate response to the Security Incident is determined by the Privacy Officer and designated personnel based upon the nature and severity of the Security Incident. Responses may include, but not be limited to, the application of sanctions against personnel, initiation of security reminders, additional training or an evaluation of the adequacy of security measures.

11.5 Any harm that is a result of the Security Incident is mitigated to the extent practicable.

11.6 All Security Incidents and their outcomes are documented in the Security Incident Log.

11.7 The Security Incident Log is reviewed on a regular basis and during the security evaluations conducted by the Hospitals to determine and ensure the adequacy of security measures and compliance with the Security Rule.

11.8 Documentation related to Security Incidents and their outcomes is retained for six years from the date of occurrence of the incident.

12. Contingency Plan

12.1 The Hospitals will maintain policies and procedures to respond to emergencies, disasters or other occurrences that damage systems that contain ePHI.

12.2 The contingency plan for ePHI includes:

- a data backup plan that includes procedures for creating, maintaining and retrieving exact copies of ePHI;
- a disaster recovery plan that includes procedures for restoring data that may be lost during a major disaster; and
- an emergency mode operation plan that provides procedures for protecting the security of ePHI while operating in emergency mode.

PART III– PHYSICAL SAFEGUARDS

13. Practice Access Controls

13.1 The Hospitals maintain practice access controls to limit the physical access to the Hospitals' practice and electronic information systems to authorized individuals.

13.2 The Hospitals maintain procedures to prevent unauthorized access to the Hospitals' practice and tampering or theft of its equipment.

13.3 To ensure that only authorized individuals have access to the Hospitals' practice and electronic information systems, access is controlled and validated by appropriate means.

13.4 Visitors to the practice should be escorted as appropriate and, if working near or with ePHI, have appropriate authorization and/or supervision.

13.5 Temporary authorization to access the Hospitals' practice and electronic information systems is granted to repair personnel or technicians during emergencies for the purpose of restoring lost data or repairing damaged equipment.

14. Workstation Use and Workstation Security

14.1 Workstations that contain or have access to ePHI are used and physically safeguarded in a manner that maximizes security and prevents unauthorized access.

14.2 Personnel are advised regarding the acceptable use of workstations (including desktops, laptops and hand-helds) that contain or have access to ePHI are provided to members of the workforce.

14.3 The Hospitals provide additional training as needed to ensure authorized users understand necessary procedures for compliance with the guidelines (for example, enabling password protected screensavers or logging off procedures).

14.4 Appropriate physical safeguards for workstations that are implemented to restrict access to authorized users may include secure locations, positioning of computer monitors, locking devices, encryption of PHI, etc.

15. Device and Media Controls

15.1 The Hospitals manages the receipt, removal and movement of hardware and Electronic Media that contain ePHI.

15.2 A record is maintained of the movement of hardware and Electronic Media that contain ePHI into, out of, and within the hospital.

15.3 A retrievable, exact backup copy of ePHI is created before moving equipment that may result in damage or the loss of data.

15.4 ePHI that is stored on the hard drives of computers or other Electronic Media is removed before the disposal or re-use of the hardware or Electronic Media.

15.5 The effective removal of ePHI from hardware or Electronic Media is verified prior to disposal or allowing re-use.

PART IV – TECHNICAL SAFEGUARDS

16. Integrity of ePHI

16.1 ePHI that is maintained in the Hospitals' information system is protected from improper alteration.

16.2 Appropriate technical mechanisms for data authentication will be used to verify the integrity of ePHI.

16.3 Appropriate procedures will be used to verify that ePHI has not been modified in an unauthorized manner.

17. Person or Entity Authentication

17.1 The Hospitals' information system verifies that a person or entity seeking access to ePHI is the one claimed.

17.2 A unique User ID is assigned to Personnel who are authorized to access the Hospitals' information system and electronic protected health information.

17.3 Personnel may not allow anyone to use their User ID to gain access to the Hospitals' information system under any circumstance without authorization from the Privacy Officer.

17.4 Personnel may not misrepresent themselves to the Hospitals' information system by using another person's User ID.

17.5 Personnel are required to follow the Hospitals' password management policies and procedures to create and safeguard their User ID to prevent unauthorized access to the Hospitals' information system.

18. Technical Access Control

18.1 Technical security measures are implemented for the Hospitals' electronic information system that maintains ePHI to allow access only to those persons or software programs that have been granted access rights.

Unique User Identification

18.2 Personnel who are authorized to access ePHI are assigned a unique User ID that enables the Hospitals' information system to identify, authenticate and track user identity.

18.3 User accounts are established that are consistent with administrative policies and procedures that authorize and grant access privileges.

18.4 Access control lists are maintained and updated as needed and technical modifications to user accounts are provided in a timely manner when access privileges are terminated or changed.

Emergency Access Procedure

18.5 Temporary access to ePHI or the Hospitals' information system is provided in emergencies.

18.6 The Hospitals' contingency plan in Section 12 of this Policy describes the Hospitals' emergency access procedures.

19. Transmission Security

19.1 The Hospitals implement technical security measures to guard against unauthorized access to ePHI that is transmitted over an electronic communications network.

19.2 ePHI may only be transmitted to authorized parties.

19.3 When ePHI must be transmitted in email communications, only the minimum amount of protected health information needed to achieve the purpose of the communication is allowed to be transmitted and must be in accordance with the Hospitals' minimum necessary disclosure policies and procedures.

19.4 A compatible, encryption method must be coordinated with the recipient of email communications containing ePHI that is transmitted over an electronic communications network.

19.5 When transmitting ePHI in email communications, the following statement or a similar statement must be included in the email as an extra precaution:

> **Confidentiality Requirement:** This email message, including any attachment(s) is for the sole use of the intended recipient(s) and may contain confidential information. Any unauthorized review, use, disclosure or distribution is strictly prohibited. If you are not the intended recipient, please immediately contact the sender by email.

PART V – REVIEW ANALYSIS, MANAGEMENT AND EVALUATION

20. Information System Activity Review

20.1 Records of information system activity are reviewed on a regular basis to prevent, detect, correct and contain security violations.

20.2 The Privacy Officer is responsible for coordinating the review of records of information system activity.

20.3 The Hospitals shall have appropriate capabilities for reviewing information system activity which may include audit logs, access reports, Security Incident Logs, paper based logs and other internal security controls and monitoring tools.

20.4 Records of information system activity are used as needed and appropriate to investigate root causes of reported or suspected Security Incidents or security violations.

20.5 Members of the workforce are periodically reminded that records of information system activity are reviewed on a regular basis.

21. Risk Analysis

21.1 The Hospitals conduct a periodic risk assessment to determine potential threats to the confidentiality, integrity and availability of ePHI.

21.2 The Hospitals have an accurate understanding of the technical and non-technical components of their respective security environment related to ePHI.

21.3 The Hospitals review and implement the standards and implementation specifications of the HIPAA Security Rule, as set forth in this Policy.

21.4 The risk assessment is retained for six years from the date completed or last updated, whichever is later.

22. Risk Management

22.1 The Hospitals select and implement security measures sufficient to reduce risks to the confidentiality, integrity and availability of ePHI to a reasonable and appropriate level.

22.2 Decisions made regarding the implementation of security measures to manage identified risks are based on the security requirements of the standards and implementation specifications of the HIPAA Security Rule.

22.3 Reasonable and appropriate risk management decisions are made taking into consideration each Hospital's size, complexity, technical capabilities, risk analysis and the costs of security measures.

22.4 Documentation of selected and implemented security measures is included in the risk analysis and management report.

22.5 The effectiveness of implemented security measures are audited during periodic evaluations of each Hospital's security environment.

PART VI– DOCUMENTATION AND AMENDMENTS

23. Documentation

23.1 The Hospitals' security policies and procedures shall be documented, reviewed periodically, and updated as necessary in response to environmental changes affecting the security of Plan, ePHI, and any changes to policies or procedures will be documented promptly.

23.2 Policies, procedures, and other documentation controlled by the Hospitals may be maintained in either written or electronic form. The Hospitals will maintain such documentation for at least six years from the date of creation or the date last in effect, whichever is later.

23.3 The Hospitals will make their policies, procedures, and other documentation available to the Privacy Officer as well as business associates or other persons responsible for implementing the procedures to which the documentation pertains.

Exhibit A

Sample Security Incident Response Report Form

Privileged and Confidential Attorney-Client Communication/Work Product

INCIDENT IDENTIFICATION INFORMATION

Date and Time of Notification:	
Incident Detector's Information:	
Name:	Date and Time Detected:
Title:	Location:
Phone/Contact Info:	System or Application:

INCIDENT SUMMARY

Type of Incident Detected:

- ☐ Denial of Service
- ☐ Malicious Code
- ☐ Unauthorized Use
- ☐ Unauthorized Access
- ☐ Unplanned Downtime
- ☐ Other

Description of Incident:

Names and Contact Information of Others Involved:

INCIDENT NOTIFICATION – OTHERS

- ☐ IS Leadership
- ☐ Security Incident Response Team
- ☐ Administration
- ☐ Other:
- ☐ System or Application Owner
- ☐ Public Affairs
- ☐ Human Resources
- ☐ System or Application Vendor
- ☐ Legal Counsel

ACTIONS

Identification Measures (Incident Verified, Assessed, Options Evaluated):

Containment Measures:

Evidence Collected (Systems Logs, etc.):

Eradication Measures:

Recovery Measures:

Other Mitigation Actions:

This form has been developed as a working tool for assessment and improvement activities; it is intended for internal use only.

Sample Security Incident Response Report Form

Privileged and Confidential Attorney-Client Communication/Work Product

EVALUATION

How Well Did Work Force Members Respond?

Were the Documented Procedures Followed? Were They Adequate?

What Information Was Needed Sooner?

Were Any Steps or Actions Taken That Might Have Inhibited the Recovery?

What Could Work Force Members Do Differently the Next Time an Incident Occurs?

What Corrective Actions Can Prevent Similar Incidents in the Future?

What Additional Resources Are Needed to Detect, Analyze, and Mitigate Future Incidents?

Other Conclusions or Recommendations:

FOLLOW-UP

Reviewed By:

- ☐ Security Officer
- ☐ Privacy Officer
- ☐ IS Department/Team
- ☐ Other

Recommended Actions Carried Out:

Initial Report Completed By:

Follow-Up Completed By:

This form has been developed as a working tool for assessment and improvement activities; it is intended for internal use only.

HEALTH INFORMATION PRIVACY POLICIES AND PROCEDURES

1. General Rule: No Use or Disclosure

It is the policy of the Community Hospital, LLC and TPG Hospital, LLC d/b/a Northwest Surgical Hospital (collectively, the "Hospitals" and each a "Hospital") to safeguard the protected health information (PHI) in accordance with the requirements of Health Insurance Portability and Accountability Act of 1996 and its implementing regulations ("HIPAA"). This regulation is also known as the Privacy Rule. We may not use (within our company and its affiliates) or disclose (outside of the company and its affiliates) PHI, except as these Health Information Privacy Policies and Procedures permit or require. "Protected Health Information" or "PHI" means information that relates to a patient's past, present, or future physical or mental condition, medical treatment, or payments for medical treatment, and that does or can be used to identify the patient. If a patient brings in PHI, such as medical records, about himself or herself, that PHI will be placed in the patient's chart and will become a part of the PHI that we keep on that patient.[1]

2. Acknowledgement

We will make a good faith effort to obtain a written acknowledgement of receipt of our Joint Notice of Privacy Practices (see Section 10) from a patient upon the initiation of the patient/resident relationship.

Community Hospital, LLC ("CH") and TPG Hospital, LLC d/b/a Northwest Surgical Hospital ("NWSH") and each of their affiliated facilities that are Covered Entities listed on Exhibit "A," the physicians and members of each of CH and NWSH clinical staff at those facilities, and the independent practitioners who practice at those facilities together form what is called an affiliated covered entity ("ACE") under HIPAA. CH and NWSH are under common ownership or control as defined in 45 CFR §§ 164.102 and 164.105(b). As an ACE, we may utilize a single shared notice of privacy practices, promulgate one consent form, designate one privacy official, and implement one set of privacy policies and procedures.

Our use or disclosure of PHI for our payment activities and healthcare operations or for the healthcare operations of the ACE is subject to the minimum necessary requirements (see Section 8), as those requirements were modified as a result of the Health Information Technology and Clinical Health Act (the "HITECH Act").

3. Authorization

Except under certain circumstances (see Sections 4, 5, and 6), we must have a current and proper written Authorization from the patient (or the patient's personal representative) before we use or disclose a patient's PHI for any purpose other than a purpose directly related to treatment, payment, or our own health care operations. The Authorization to Disclose Protected Health Information is HP Form 02. We will act in accordance with an Authorization that meets the applicable legal requirements.

a) Authorization Revocation – A patient may revoke an Authorization at any time by written notice to the Privacy Officer ("PO"). We will not rely on an Authorization we know has been properly revoked. A Revocation of Authorization to Disclose Protected Health Information form is HP Form 03.

b) Authorization Expiration – We will not rely on an Authorization we know has expired.

c) Authorization from Another Provider – We will use or disclose PHI as permitted by a valid Authorization we receive from another healthcare provider.

[1] Psychotherapy Notes are defined in the Privacy Rule as 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 patient's medical record. Psychotherapy Notes exclude medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date. If a patient brings in Psychotherapy Notes from another provider, those will be placed with the Psychotherapy Notes that we keep on the patient and will be kept separate from the rest of the patient's medical record we maintain.

As the disclosing entity, we are obligated to make our own "minimum necessary" determination with respect to a request for PHI from another health care provider.

4. Permitted Use or Disclosure Without Authorization (with Oral or Written Agreement)

We may use or disclose a patient's PHI in the following situations without the need for a written authorization, with the patient's Oral Agreement or Written Agreement**,** or if the patient is unavailable, subject to all applicable requirements of the Privacy Rule:

1. For a Hospital directory (subject to the patient's right to "opt-out" and limited to "directory information");
2. To individuals involved in the patient's care or payment for the patient's care for involvement and notification purposes, including if the patient is deceased (subject to the patient's right to object or request a restriction on use and disclosure); and
3. For disaster relief efforts (subject to the patient's right to object or request a restriction on use and disclosure).

If a patient wants to restrict disclosures of his or her protected health information to someone who is involved in the patient's care or payment for the patient's care, such as a family member or a close personal friend, the patient may request a restriction. A Request to Restrict Uses and Disclosures of Protected Health Information form is HP Form 04.

We may use professional judgment and our 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 medical supplies, X-rays, or other similar forms of PHI.

5. Permitted Use or Disclosure Without Authorization or Oral or Written Agreement

We may use or disclose a patient's PHI in the following situations, without Authorization or an Oral Agreement or a Written Agreement**,** provided procedures specified in the Privacy Rule are followed:

1. For treatment and services;
2. For payment;
3. For our health care operations;
4. To business associates;
5. To report abuse, neglect, or domestic violence to a government agency;
6. For certain research projects;
7. To create "limited data sets" under certain circumstances;
8. As required by law;
9. To avert a serious threat to health or safety;
10. To the United States or a foreign military;
11. As authorized by state worker's compensation laws;
12. For public health disclosures;
13. For health oversight activities;
14. For legal proceedings, lawsuits, and other legal actions;
15. For law enforcement purposes;
16. To coroners, medical examiners, and funeral directors;
17. For national-security and intelligence activities;
18. For protective services for the United States president, other authorized persons, or foreign heads of state;
19. To correctional institutions regarding inmates or to a law enforcement official regarding someone in his/her lawful custody; and
20. For organ, eye, or tissue donation purposes.

6. Required Disclosures

We will disclose PHI to a patient (or to the patient's personal representative) to the extent that the patient or the patient's personal representative has a right of access to the PHI (see Section 11); we will not disclose to a personal representative we reasonably believe may be abusive to a patient any PHI we reasonably believe may promote or further such abuse, and we will make reports of such abusive behavior as required by law.

We will also disclose PHI to the U.S. Department of Health and Human Services ("HHS") on request for complaint investigation or compliance review.

7. Verification of Identity and Authority

We will always verify the identity of any patient, and the identity and authority of any patient's personal representative, government, or law enforcement official, or other person, unknown to us, who requests PHI before we will disclose the PHI to that person, including whether the individual may be or was a patient or resident of a practice that is a Covered Entity. Examples of appropriate identification include photographic identification card, government identification card or badge, and appropriate document on government letterhead.

If the person is not the patient, we will obtain evidence of authority that the person is entitled to receive the PHI pursuant to the Privacy Rule.

If the identity and authority of the requesting individual cannot be verified, the individual will be informed that a new request must be completed and notarized and that we must be able to verify the person's identity and authority in accordance with the Privacy Rule before any PHI is disclosed. We will document the incident and how we responded.

8. Minimum Necessary

We will make reasonable efforts to request of another Covered Entity, and to use and disclose, only the minimum necessary PHI to accomplish the intended purpose.

There is no minimum necessary requirement for uses and disclosures of or requests for PHI by one another in CH, NWSH or our affiliated facilities or by a health care provider for treatment purposes; permitted or required disclosures of PHI to, or for disclosures of PHI requested or authorized by, a patient; disclosures of PHI to HHS for compliance reviews or complaint investigations; disclosures of PHI required by law; or uses or disclosures of PHI required for compliance with the HIPAA Administrative Simplification Rules.

a) Limited Data Set. If the minimum necessary requirement does apply to the situation, then as an initial matter, workforce members must always consider whether a Limited Data Set (as defined in the Privacy Rule) will provide sufficient PHI for the intended purpose of the use or disclosure; if so, that is the only PHI that may be used or disclosed.

b) Criteria for Minimum Necessary for Uses, Disclosures and Requests by us Where Limited Data Set Will Not Suffice.

i. Routine or Recurring Requests or Uses and Disclosures – We will follow the policies and procedures that we adopt to limit our routine or recurring requests for or uses and disclosures of PHI to the minimum reasonably necessary for the purpose.

ii. Non-Routine or Non-Recurring Requests or Disclosures – No non-routine or non-recurring request for or disclosure of PHI will be made until it has been reviewed on a patient-by-patient basis against our criteria to ensure that only the minimum necessary PHI for the purpose is requested or disclosed.

c) Other's Requests – We must determine what constitutes the minimum necessary amount of PHI.

d) Entire Record – We will not use, disclose, or request an entire record, except as permitted in these Health Information Privacy Policies & Procedures or in standard protocols that we adopt reflecting situations when it is necessary.

e) Minimum Necessary Workforce Use, Disclosure, or Request – Workforce members will use, disclose, and request only the minimum necessary PHI needed to perform their duties, except that this rule does not apply to PHI needed to be used, disclosed, or requested for treatment purposes.

9. Business Associates

We will obtain satisfactory assurance in the form of a written contract that our Business Associates will appropriately safeguard and limit their use and disclosure of the PHI we disclose to them.

These Business Associate requirements are not applicable to our disclosures to a health care provider for treatment purposes. We have developed one or more form Business Associate Agreement(s) that contain the terms that federal law requires be included in each Business Associate contract. An example agreement is available as Exhibit "B".

If we learn that a Business Associate has materially breached or violated its Business Associate Agreement with us, we will take prompt, reasonable steps to see that the breach or violation is cured. If the Business Associate does not promptly and effectively cure the breach or violation, we will terminate our contract with the Business Associate, or if contract termination is not feasible, report the Business Associate's breach or violation to HHS.

10. Joint Notice of Privacy Practices

We will maintain a Joint Notice of Privacy Practices as required by the Privacy Rule. Our Joint Notice of Privacy Practices contains the terms that federal law requires. A copy of the Notice is attached as Exhibit "C".

a) Our Notice – We will use and disclose PHI only in conformance with the contents of our Joint Notice of Privacy Practices. We will promptly revise our Joint Notice of Privacy Practices whenever there is a material change to our uses or disclosures of PHI, to our legal duties with respect to PHI, to the patients' rights with respect to PHI, or to other privacy practices that render the statements in our current Notice no longer accurate. Except when required by law, a material change to any term of our Joint Notice of Privacy Practices will not be implemented prior to the effective date of the Notice in which such material change is reflected.

b) Distribution of Our Notice – We will provide our Joint Notice of Privacy Practices to any person who requests it and to each patient no later than the date of our first service delivery.

We will have our Joint Notice of Privacy Practices available for patients to take with them. We will also post our Joint Notice of Privacy Practices in a clear and prominent location where it is reasonable to expect patients seeking services from us will be able to read the Notice. We will also post our Joint Notice of Privacy Practices on each Hospital's website.

c) Acknowledgement of Notice – We will make a good faith effort to obtain from the patient a written acknowledgement of receipt of our Joint Notice of Privacy Practices. Our Acknowledgement of Receipt of Notice of Privacy Practices is included on our Conditions of Admission and Authorization for Medical Treatment which each patient must complete prior to admission. If we cannot obtain written acknowledgement from the patient, we will document our attempt and the reason why the written Acknowledgement was not signed by the patient.

11. Patients' Rights

We will honor the rights of patients regarding their PHI.

a) Designated Records Set - The HIPAA Privacy Rule requires that patients be permitted to request access and amendment to their PHI that is maintained in a Designated Record Set (DRS). DRS is a group of records maintained by or for the Hospital that consists of the medical records and billing records about a patient and is used, in whole or in part, by or for the Hospital to make decisions about the patient. The term record means any item, collection, or grouping of information that includes PHI and is maintained, collected, used, or disseminated by or for the patient.

The Hospital maintains the following as the Designated Record Set:

i. The Patient's Medical Record,
ii. The Patient's Business Office File, and
iii. The Patient's Personal Health Records.

The Patient Medical Record includes, at a minimum, the following:

- Activity documentation
- Admission/readmission documentation
- Advance directives
- Assessments, flow sheets
- Care plan
- Informed consent
- History and physical exams and other related hospital records
- Minimum Data Set
- Medication and treatment records
- Nursing documentation/progress notes
- Nutritional services documentation
- Physician and professional consultant progress notes
- Physician's orders
- Rehabilitative and restorative therapy records
- Reports from lab, x-ray and other diagnostic tests
- Face sheet
- Social service documentation

Excluded from the Medical Record are source data, including photographs, films, monitoring strips, videotapes, digital recordings of procedures, slides, worksheets and daily communication sheets, and shadow files or charts, unless such data is used to make decisions related to the Patient's care.

If records from other providers are used by the Hospital to make decisions related to the care and treatment of the Patient, then these records are considered part of the Designated Record Set as well as the Medical Record, e.g., history and physical, discharge summary and labs from previous acute care hospitalization.

The Patient's Business Office File includes, at a minimum, the following:

- Admission documents
- Acknowledgement of receipt of the Hospital's Notice of Privacy Practices
- Correspondence relating to coverage and payment from insurance companies, health plans, Medicare, Medicaid and other payor sources
- Patient claim information, including claim, remittance, eligibility response, and claim status response
- Statements of account balance
- Collection activity documents and correspondence

Personal Health Records consist of the Patient's personal health information provided to the Hospital by the Patient. If such records are used by the Hospital to make health care related decisions, provide care services, or document observations, actions or instructions, then the records will be considered part of the Designated Record Set.

The following are excluded from the Designated Record Set: Administrative data, such as audit trails, reports, indexes, appointment schedules and practice guidelines. Also excluded are incident reports, quality assurance or infection control data, peer review information, vital certificate worksheets, and derived data such as accreditation reports, anonymous Patient data for research purposes, public health records and statistical reports.

The Designated Record Set is to be retained according to state and federal regulations and following Hospital or Hospital retention procedures.

b) Access – With rare exceptions, patients have the right to request access to their PHI that we or our Business Associates maintain about them.

No PHI will be withheld from a patient or his/her authorized personal representative (authority of the personal representative must be confirmed under the Privacy Rule and applicable state law) seeking access unless we confirm that the information may be withheld according to the Privacy Rule or in accordance with other applicable state or federal law.

Under certain circumstances, we may offer to provide a summary of the information in the chart. The patient must agree in advance to receive a summary and to any fee we will charge for providing the summary.

After receiving a request for access, we will contact our Business Associates to retrieve any PHI they may have on the patient.

Requests for access to patient records must be in writing and submitted to the PO. A Request for Access to Inspect or Copy Protected Health Information form is HP Form 05. The form in which the patient would like to receive the records must be specified in the request (e.g., paper or electronic). Access to the records will be provided in the form requested if it is readily producible in such format. If the form requested is not readily producible, records must be provided in readable form agreed to by the individual. If a patient or his/her authorized representative requests records to be provided in electronic format, the data must be encrypted. If the PO receives such a request, the PO must contact IT for assistance. If the patient/authorized representative requests that a copy be transmitted to a person designated by the patient/authorized representative, the request must be in writing.

If possible, we must act on requests for access to records within 30[2] days of the request. If we are unable to act on a request within such 30-day period, the timeframe may be extended an additional 30 days one time

[2] Under Section 42 CFR 483.10, a current patient or the legal representative of a current patient has the right, (i) upon oral or written request, to access all records pertaining to the patient including current clinical records within

by providing written notice to the patient or the patient's personal representative within the original timeframe to include the reasons for the delay and date by which access will be provided.

If the requested information is not available and the whereabouts are unknown, this information will be documented on the written request and returned to the individual with a copy filed in the patient record.

c) Charges for copying – By Oklahoma statute, we may charge you $.50 per page, plus our postage costs. If your record contains any item that requires a photographic process to copy, such as a x-ray or photograph, we may charge you $5.00 per image. If we can deliver records electronically, we will provide the records in electronic form and will charge $0.30 per page, up to a maximum of $200 per request.

d) Amendment – Patients have the right to request an amendment or addendum to their PHI and other records for as long as we maintain them. Requests to amend PHI, together with an explanation therefor, must be in writing and submitted to the PO. A Request to Amend Protected Health Information form is HP Form 06.

We must act on a request for an amendment no later than 60 days after receipt or the request if we are able to do so. If we are not able to respond to the request within such 60-day period, we may extend the time for us to act by no more than 30 days. We may have only one such extension of time, and we must inform the patient or his/her authorized representative, as applicable, in writing within the original 60-day timeframe of the reasons for the delay and the date by which we will act on the request.

We may deny a request to amend PHI or records if: (i) we did not create the information (unless the patient provides us a reasonable basis to believe that the originator is not available to act on a request to amend); (ii) we do not have the information as part of our health and billing records kept by or for us; (iii) we believe the information is accurate and complete; or (d) we are otherwise permitted to deny a request for access to the information pursuant to the Privacy Rule.

We will follow all procedures required by the Privacy Rule for denial or approval of amendment requests. We will not, however, physically alter or delete existing notes in a patient's chart. We will inform the patient when we agree to make an amendment, and we will contact our Business Associates to help assure that any PHI they have on the patient is appropriately amended. We will contact any individuals whom the patient requests we alert to any amendment to the patient's PHI. We will also contact any individuals or entities of which we are aware that we have sent erroneous or incomplete information and who may have acted on the erroneous or incomplete information to the detriment of the patient.

When we deny a request for an amendment, we will make any future disclosures of the contested information in a way acknowledging the contest in accordance with the Privacy Rule.

e) Denial of a Request for Access or Amendment - If a request for access or amendment is denied, notice to the patient must be made in writing and must include the reason for denial, a description of how a complaint may be filed with the PO, and a description of how a complaint may be filed with the Office of Civil Right ("OCR") at HHS (see Section 12b).

f) Disclosure Accounting – Patients have the right to an accounting of certain disclosures we made of their PHI within the 6 years prior to their written request. Requests for an accounting of disclosures of PHI must be in writing and submitted to the PO. A Request for an Accounting of Disclosures of Protected Health Information form is HP Form 07. Each disclosure we make that we are required to account for (see next paragraph), must be documented showing the date of the disclosure, what was disclosed, the purpose of the disclosure, and the name and (if known) address of each person or entity to whom the disclosure was made. The Authorization permitting the disclosure (if required) or other documentation describing the disclosure must be included in the patient's record and retained for at least six years from the date it was created or, in the case of an authorization, for at least six years from the date that it was last in effect. In order to enable us to fulfill our obligation to account for these disclosures, we will either use the patient's chart or our Accounting of Disclosures of Protected Health Information form. This form is Exhibit "D".

---

24 hours (excluding weekends and holidays); and (ii) after receipt of the patient's records for inspection, to purchase at a cost not to exceed the practice standard, photocopies of the records or any portions of them upon request and two working days' advance notice to the practice.

We must act on a request for an accounting no later than 60 days after receipt or the request if we are able to do so. If we are not able to respond to the request within such 60-day period, we may extend the time for us to act by no more than 30 days. We may have only one such extension of time, and we must inform the patient or his/her authorized representative, as applicable, in writing within the original 60-day timeframe of the reasons for the delay and the date by which we will act on the request.

We are not required to account for disclosures we made: (i) to carry out treatment, billing, and health care operations; (ii) to the patient (or the patient's personal representative); (iii) incident to a permitted or required use or disclosure; (iv) to parties who receive the patient's information pursuant to a valid authorization; (v) to those who request the patient's information through a Hospital directory (unless the patient has elected to "opt out"); (vi) to the patient's family members, other relatives, or friends who are involved in the patient's care, or who otherwise need to be notified of the patient's location, general condition, or death (unless the patient has requested a restriction); (vii) for national-security or intelligence purposes; (viii) to correctional institutions or law enforcement officials regarding inmates; or (ix) as part of a Limited Data Set.

We will temporarily suspend the accounting of any disclosures when requested to do so by health oversight agencies or law enforcement officials in accordance with Privacy Rule requirements.

We may charge for any accounting that is more frequent than every 12 months, provided the patient is informed of the fee before the accounting is provided.

We will contact our Business Associates to assure we include in the accounting any disclosures made by them for which we must account.

g) Restrictions on Uses or Disclosures – Patients have the right to request us to restrict uses or disclosures of their PHI, including for treatment, payment, or health care operations. Patients also have the right to request us to restrict uses or disclosures of their protected health information to someone who is involved in their care or payment for their care such as family members or close personal friends. Requests for restrictions on uses or disclosures of PHI must be in writing and submitted to the PO. A Request to Restrict Uses and Disclosures of Protected Health Information form is HP Form 04. We have no obligation to agree to the request, except the PO must agree to a request to restrict disclosures to a health plan for the purposes of payment or health care operations if the information to be restricted pertains solely to a health care item or service that has been paid for out of pocket in full and the disclosure is not otherwise required by law. If we do agree to a request, we will comply with our agreement (except in an appropriate medical emergency).

We may terminate an agreement restricting use or disclosure of PHI (unless the restriction pertains to services paid in full out-of-pocket; see above) by a written notice of termination to the patient if—

- The patient agrees to or requests the termination in writing;
- The patient orally agrees to the termination and the oral agreement is documented; or
- We inform the patient in writing we are terminating our agreement, except that such termination is only effective with respect to protected health information created or received by us after we have informed the patient of the termination of the restrictions.

We will document in the patient's chart any such agreed-to restrictions.

h) Requests for Alternative Communications – Patients have the right to request that communications be made to alternate locations (e. g., at work instead of at a home address) or by alternative means (e.g., by phone instead of mail). Requests for alternative communications must be in writing and submitted to the PO. A Request for Alternative Communications form is HP Form 08. We must accept and accommodate reasonable requests for patient communications to alternative locations or by alternative means.

i) Applicability – We will be aware of and respect these patients' rights regarding their PHI.

12. Workforce Training and Management, Complaint Procedures, Data Safeguards, Administrative Practices

a) Workforce Training and Management

Training – The PO will train all members of the workforce in the Hospital, as necessary and appropriate for them to carry out their functions.

After these policies and procedures are adopted, the PO will train each new workforce member within a reasonable time after the member starts. We will also retrain each workforce member whose functions are affected either by a material change in our Health Information Privacy Policies and Procedures or in the member's job functions, within a reasonable time after the change.

Sanctions, Discipline, and Mitigation – We will develop, document, disseminate, and implement appropriate discipline policies for workforce members who violate our Health Information Privacy Policies and Procedures, the Privacy Rule, or other applicable federal or state privacy law.

Workforce members who violate our Health Information Privacy Policies and Procedures, the Privacy Rule, or other applicable federal or state privacy law will be subject to disciplinary action, possibly up to and including termination of employment or status as a volunteer, consultant or vendor.

b) Complaints – We will implement procedures for individuals to complain about our Health Information Privacy Policies and Procedures or our compliance with them or our compliance with the Privacy Rule. We will also implement procedures to investigate and resolve such complaints.

An individual may lodge a written complaint with one of our facilities by filing a Complaint about Uses and Disclosures of Protected Health Information with the Hospital's PO. The form is HP Form 09. Upon receipt of a Complaint, the PO must take action to investigate the complaint and resolve any substantiated allegations.

An individual may also file a written complaint with the U.S. Department of Health and Human Services, Office for Civil Rights ("OCR"). An individual must file a complaint with the OCR within 180 days of when he or she knew that the act or omission complained of occurred. The OCR may extend the 180-day period for "good cause." The OCR recommends that an individual use the OCR ***Health Information Privacy Complaint Form Package*** to file a complaint with the OCR. This package, together with other helpful information on how to file a complaint with the OCR, is available on the OCR website at http://www.hhs.gov/ocr/privacy/hipaa/complaints/. An individual may file a written complaint with the OCR, either on paper or electronically, by mail, fax, or e-mail. To submit a complaint to the OCR by mail or fax, an individual must submit it to the regional office where the alleged violation took place. The contact information for the OCR regional offices is listed in HP Form 09. To submit an electronic complaint with the OCR, an individual should go to the OCR's website at: http://www.hhs.gov/ocr/privacyhowtofile.html.

We will not retaliate against any person who makes a Complaint in good faith.

c) Data Safeguards and Reporting of Breaches of Confidentiality – We will strengthen these Health Information Privacy Policies and Procedures with such additional policies and procedures as are needed to have reasonable and appropriate administrative, technical, and physical safeguards in place to ensure the integrity and confidentiality of the PHI we maintain.

We will take reasonable steps to limit incidental uses and disclosures of PHI made incidental to an otherwise permitted or required use or disclosure.

All workforce members are required to report ***immediately*** to the PO any suspected or known violation of these Health Information Privacy Policies and Procedures or the Privacy Rule, or any case in which a patient's PHI might have been compromised. Examples include:

- Misdirected e-mails containing PHI;
- Unencrypted lost or stolen laptops, PDAs, flash drives, or thumb drives with PHI on them;

- throwing away handwritten files or notes, including post-its, on a patient chart without shredding them first; or
- faxing patient information to an incorrect fax number.

The PO will conduct an investigation of the alleged breach of confidentiality, and CH and NWSH and their affiliated entities that are Covered Entities listed on Exhibit "A" will abide by the Data Breach Notification Rule as amended, 45 CFR Part 160 and Part 164, Subpart D, which is incorporated herein by reference, to the extent that such breach constitutes a breach of unsecured protected health information, as well as any other state or federal notifications laws that may apply to the information breach.

d) Documentation and Record Retention – We will maintain in written or electronic form all documentation required by the Privacy Rule for six years from the date of creation or when the document was last in effect, whichever is greater, or such longer period of time which may be required under state law.

13. State Law Compliance

Each affiliated Hospital will comply with the privacy laws of each state that has jurisdiction over it, or its actions involving PHI, that provide greater protections or rights to patients than the Privacy Rule. These types of laws include, but are not limited to:

a) Free copies or specified copying charges for patient records (see Section 11(b)).

b) Privileges. Patients may invoke a provider – patient privilege to prevent evidence from being introduced in court against them.

c) Certain Conditions. Many states have specific requirements that must be followed when disclosing patient information about sexually transmitted diseases, HIV/AIDs, mental health, and substance abuse, which might impose additional requirements on an authorization form or which might require a notice to be sent to the recipient of the information warning against re-disclosure. When disclosing patient records containing such PHI, please consult with the PO.

d) Breach Notification. Many states have specific requirements that must be followed regarding notifications following a breach of security involving sensitive personal information.

Any questions you have regarding state law compliance should be discussed with the PO before you act.

14. HHS Enforcement

We will give HHS access to our facilities, books, records, accounts, and other information sources (including individually identifiable health information without patient authorization or notice) during normal business hours (or at other times without notice if HHS presents appropriate lawful administrative or judicial process).

We will cooperate with any compliance review or complaint investigation by HHS, while preserving our rights.

15. Privacy Officer

We have designated a PO as required by the Privacy Rule. The contact for our PO follows.

Diana Waddell
3100 S.W. 89th Street, Oklahoma City, OK 73159
(405) 602-8163

EXHIBIT A

AFFILIATED COVERED ENTITIES

Community Hospital, 3100 S.W. 89th Street, OKC, OK 73159 • 405-602-8100
Community Hospital MRI Center, 3100 S.W. 89th Street, OKC, OK 73159 • 405-605-2660
Community Hospital Outpatient Surgery, 6205 N. Santa Fe, Suite 100, OKC, OK 73118 • 405-419-5566
Community Hospital Outpatient Therapy
Quail • 14024 Quail Pointe Drive, OKC, OK 73134 • 405-340-2025
North • 801 N.W. 63rd St., OKC, OK 73116 • 405-879-9997
South • 10001 S. Western Ave., Suite 102, OKC, OK 73139 •405-691-5434
South /Hand• 10001 S. Western Ave., Suite 204, OKC, OK 73139 • 405-427-3752
Northwest Surgical Hospital, 9204 North May Avenue, OKC, OK 73120 • 405-848-1918
Northwest Surgical Hospital Lakepointe Imaging, 10914 Hefner Pointe Drive, Suite 100, OKC, OK 73120 • 405-488-7226

EXHIBIT B

BUSINESS ASSOCIATE AGREEMENT

[See Attached]

EXHIBIT C

JOINT NOTICE OF PRIVACY PRACTICES

[See Attached]

EXHIBIT D

ACCOUNTING OF DISCLOSURES OF PROTECTED HEALTH INFORMATION

[See Attached]

REQUEST FOR ACCESS TO INSPECT OR COPY PROTECTED HEALTH INFORMATION

You have the right to request access to inspect or obtain a copy of your protected health information that we maintain about you. Your request must be made in writing.

If possible, we must act on your request for access no later than 30 days after receipt of your request. If we are unable to act on your request within this 30-day period, we may extend the time for such action by no more than 30 days. We may have only one such extension of time, and we must tell you in writing within the original 30-day timeframe the reasons for the delay and the date by which we will complete our action on your request.

We may grant or deny your request for access, in whole or in part. If we grant your request, we will arrange with you a convenient time and place to inspect or obtain a copy of your protected health information, or we will mail a copy at your request. In the alternative, if you agree in advance, we may provide you with a summary of your protected health information in lieu of providing access. If we deny your request for access, we will notify you in writing of the basis for our denial. We will also provide you with information regarding your right, under certain circumstances, to have our denial reviewed by a licensed health care professional who is designated by us, but who did not participate in our original decision to deny access. We will also tell you how to file a complaint regarding our denial with us or with the Secretary of the U.S. Department of Health and Human Services.

If your protected health information is in electronic form, you may request an electronic copy of such information and indicate the particular form and format in which you want to receive it. We will comply if we can readily produce the information in such form and format. If not, we will provide it in such readable electronic form and format as you and we mutually agree upon. You may also request that we transmit the copy of your protected health information to another person designated by you. Such request must be made in writing.

If you request a copy of your protected health information or agree to a summary, we may charge you a reasonable, cost-based fee that includes only our labor costs and costs of supplies used in creating the copy (whether paper or electronic), postage (if you request the information be mailed to you), and costs in preparing the summary (if you have agreed to a summary).

Patient's Name (print): _____

Patient's Date of Birth: _____

I am requesting (**check applicable boxes**): the right to inspect ☐ and/or a copy of ☐ the protected health information about the patient identified above ("Patient") maintained by Community Hospital, LLC or TPG Hospital, LLC d/b/a Northwest Surgical Hospital, as applicable (the "Hospital"). I understand I do not have the right to inspect or copy psychotherapy notes or information compiled in anticipation of a legal or administrative action or proceeding or information restricted by law.

I would like the requested information to be made available to me in the following form (**check applicable box**): paper form ☐ or electronic form ☐; however, I understand if the requested form is not readily producible, a readable form that we mutually agree upon will be provided.

☐ **(check box if applicable)** I want you to transmit a copy of the Patient's protected health information to the following person at the following site or location:

Name: _____

Location: _____

_____

I am interested in the Patient's protected health information described below for the period of _____ _____until_____:

☐ I want to inspect the Patient's protected health information at the Hospital.

☐ I want a copy of the Patient's protected health information at the Hospital. I understand that there will be a reasonable, cost-based fee that includes only the labor costs and costs of supplies used in creating the copy (whether paper or electronic).

☐ I want to pick up the copy at the Hospital.

☐ I want the Hospital to send me the copy using my current contact information set forth below. I understand that I will pay the cost for postage.

☐ I want the Hospital to send me a written summary of the Patient's protected health information using my current contact information set forth below. I understand that the summary will cost $_____, plus the cost for postage.

This form must be signed by either the Patient or by the Patient's personal representative.

If this form is signed by the Patient's personal representative, please provide a copy of the document naming the personal representative and provide a description of the personal representative's authority to act on behalf of the Patient:_____

_____

_____ Date:_____
Signature of Patient or Patient's Personal Representative

Current Contact Information for Patient or Personal Representative signing this form:

Name (print):_____

Address:_____

Telephone Number:_____

Email:_____

Submit this form to the Hospital's Privacy Officer.

This form should be placed in the patient's medical record.

REQUEST FOR AN ACCOUNTING OF DISCLOSURES OF PROTECTED HEALTH INFORMATION

You have the right to request an accounting of certain types of disclosures of your protected health information made by us in the six years prior to the date on which the accounting is requested. Your request must be made in writing.

We must act on your request for an accounting no later than 60 days after receipt of your request. Notwithstanding the foregoing, if we are unable to respond to your request within 60 days, we may extend the time for us to act by no more than 30 days. We may have only one such extension of time and we must tell you in writing within the original timeframe the reasons for the delay and the date by which we will act on your request.

Our accounting of the disclosures of your protected health information must generally include the following for each disclosure: (a) the date of the disclosure, (b) the name and (if known) the address of the entity or person who received the protected information, (c) a brief description of the protected health information disclosed, and (d) a brief statement of the purpose of the disclosure. We will document disclosures that must be accounted for using the "Accounting of Disclosures of Protected Health Information" form or a substantially similar form.

We must provide the first accounting to you in any 12-month period without charge. We may charge you a reasonable fee for each subsequent request for an accounting by you within the same 12-month period. If you notify us before we prepare our response to your request, you may withdraw or modify your request for an accounting in order to avoid or reduce our fee.

Patient's Name (print):_____

Patient's Date of Birth:_____

☐ I request an accounting of the disclosure of protected health information of the patent identified above ("Patient") made by Community Hospital, LLC or TPG Hospital, LLC d/b/a Northwest Surgical Hospital, as applicable (the "Hospital"):

☐ for the six years preceding the date of this request

☐ for the period of time from _____ to _____

Please provide the requested accounting summary to the following:

Name (print):_____

Address: _____

Telephone Number: _____

Email:_____

This form must be signed by either the Patient or by the Patient's personal representative.

If this form is signed by the Patient's personal representative, please provide a copy of the document naming the personal representative and provide a description of the personal representative's authority to act on behalf of the Patient:_____

_____

_____ Date:_____

Signature of Patient or Patient's Personal Representative

Current Contact Information for Patient or Personal Representative signing this form:

Name (print):_____

Address: _____

Telephone Number: _____

Email:_____

Submit this form to the Hospital's Privacy Officer.

This form should be placed in the patient's medical record.

REQUEST TO AMEND
PROTECTED HEALTH INFORMATION

You have the right to request that we amend your protected health information maintained by us. Your request must be made in writing and you must provide a reason to support the requested amendment.

We must act on your request for an amendment no later than 60 days after receipt of your request. Notwithstanding the foregoing, if we are unable to respond to your request within 60 days, we may extend the time for us to act by no more than 30 days. We may have only one such extension of time and we must tell you in writing within the original timeframe the reasons for the delay and the date by which we will act on your request.

We may grant or deny your request for an amendment, in whole or in part. If we grant your request, we will make the requested amendment by amending or appending your protected health information (we cannot delete protected health information from your records). We will also make reasonable efforts to inform and provide the amendment to persons identified by you and by us as having received your protected health care information and needing the amendment. If we deny your request for an amendment, we will notify you in writing of the basis for our denial. We will also provide you with information on your right to: (i) submit a written statement disagreeing with our denial, (ii) request that we provide your original request for an amendment and our denial with any future disclosures of your protected health information that is the subject of the amendment, and (iii) file a complaint regarding our denial with us or with the Secretary of the U.S. Department of Health and Human Services.

Patient's Name (print):_____

Patient's Date of Birth:_____

I request Community Hospital, LLC or TPG Hospital, LLC d/b/a Northwest Surgical Hospital, as applicable (the "Hospital"), to amend the protected health information maintained by the Hospital on the patient identified above ("Patient"), as follows:

_____
_____
_____
_____
_____
_____
_____
_____

I am requesting the Hospital to amend the Patient's protected health information for the following reason(s):

_____
_____
_____
_____
_____
_____
_____
_____

If you accept the requested amendment of the Patient's protected health information, I want you to notify the following individuals and/or entities of the amendment:

Name	Contact Information

This form must be signed by either the Patient or by the Patient's personal representative.

If this form is signed by the Patient's personal representative, please provide a copy of the document naming the personal representative and provide a description of the personal representative's authority to act on behalf of the Patient:_____

_____

_____ Date:_____

Signature of Patient or Patient's Personal Representative

Current Contact Information for Patient or Personal Representative signing this form:

Name (print):_____

Address:_____

Telephone Number: _____

Email: _____

Submit this form to the Hospital's Privacy Officer.

This form should be placed in the patient's medical record.

Community Hospital, LLC **HP Form 04**
TPG Hospital, LLC d/b/a Northwest Surgical Hospital

REQUEST TO RESTRICT USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION

Each time you receive care or treatment at our facility, a record of your visit is made. Such record includes protected health information ("PHI") such as your symptoms, examination, test results and diagnoses. In order to bill your health plan for care and treatment provided to you, the facility must provide your health plan with certain PHI about you.

You have the right to request that the facility not share your PHI with your health plan for specific items or services, so long as you pay for such items or services out of pocket in full. If you would like to restrict the facility's disclosure of PHI to your health plan, you may do so by completing this form. If you would like to request a similar restriction of PHI maintained by any other health entity, a separate request must be submitted in writing to that provider.

I request that the facility indicated below not disclose my Protected Health Information ("PHI") to the health plan indicated below (my "Health Plan") regarding the specific healthcare item(s) or service(s) listed below, for the specific date(s) of service listed below (the "Services"):

Facility Name & Address: _____

My Health Plan: _____

Services for which I'm requesting a restriction and for which I'm paying out of pocket in full:

Item or Service	Date(s) of Service

I understand that I must pay out of pocket the full amount for the Services, and if I do not (or if my payment is denied or otherwise fails in any way) I agree that the Facility may bill my Health Plan for the Services in its usual manner (and provide my Health Plan with necessary PHI for such payment purposes). Any amount I self-pay today is based on an estimate, and may not be the amount ultimately due for the Services. If I fail to pay any balance due within 30 days of my receipt of a bill from the Facility, I agree that the Facility may bill my Health Plan in its usual manner (and provide my Health Plan with necessary PHI for such payment purposes).

I further understand that (i) **I am responsible for communicating any restriction request to my other health care providers involved in the Services, including, but not limited to, any physicians who participate in my care (e.g., Emergency Department physician, attending and consulting physicians, radiologists, pathologists and anesthesiologists, etc.) and any "downstream" providers, such as any home health agency or pharmacy to which I'm referred**, (ii) this restriction does not cover any item(s) or service(s) rendered as a result of any complications arising from the Services, and (iii) this request applies to disclosures for payment and healthcare operations purposes and does not apply to disclosures for treatment purposes or for disclosures required by law. I agree that the Facility is not responsible for disclosures made prior to its receipt of this request and payment in full, and I further understand any amounts self-paid by me will not be communicated to my Health Plan, so such self-paid amounts will not apply to any of my annual deductibles or out-of-pocket thresholds. I further understand and agree that this restriction applies to the above listed date(s) of service only and that the Facility or my other healthcare providers may reference the Services provided on these dates and associated results in the medical record documentation of my future care or treatment. If I want such PHI withheld from my Health Plan, then I must submit a similar request in connection with such future care or treatment and pay for such future services out of pocket in full.

_____ _____ _____
Signature of Patient (or Name of Patient if Signed Below) Request Date Request Time

_____ _____
Address Telephone

If (i) the patient is a minor, the patient's parent or guardian should consent by signing below, or (ii) if the patient is an adult but unable to consent for himself or herself, then the patient's guardian, legal representative, attorney-in-fact, surrogate or proxy should consent on the patient's behalf by signing below:

_____ _____
Signature of Representative *Telephone*

_____ _____
Print Name *Relationship to Patient*

Facility Use Only:

_____ _____ _____ $_____
Facility Representative Date Received Time Received Estimate

Services Paid in Full?
□ **Yes:** Restriction Accepted
□ **Pending:** Balance Due Date _____
□ **No:** Restriction Denied

Community Hospital, LLC **HP Form 08**
TPG Hospital, LLC d/b/a Northwest Surgical Hospital

REQUEST FOR ALTERNATIVE COMMUNICATIONS

You have the right to request to receive communications of your protected health information from us by an alternative means or at an alternative location. Your request must be made in writing. We must accept and accommodate reasonable requests to receive communications by an alternative means or at an alternative location. However, we may condition our acceptance and accommodation on:

- our ability to continue to receive timely payment; and
- our ability to use the alternative address or other method of contact based on the information you provide to us.

Patient's Name (print):_____

Patient's Date of Birth:_____

I request Community Hospital, LLC or TPG Hospital, LLC d/b/a Northwest Surgical Hospital, as applicable (the "Hospital"), to communicate the protected health information about the patient identified above ("Patient") using the following alternative location or alternative means of communication:

☐ Mail ☐ Telephone ☐ E-Mail ☐ Other

Alternative Mailing Address:_____

Alternative Telephone Number:_____

Alternative E-Mail Address:_____

Other:_____

This form must be signed by either the Patient or by the Patient's personal representative.

If this form is signed by the Patient's personal representative, please provide a copy of the document naming the personal representative and provide a description of the personal representative's authority to act on behalf of the Patient:_____

_____

_____ Date:_____
Signature of Patient or Patient's Personal Representative

Current Contact Information for Patient or Personal Representative signing this form:

Name (print):_____

Address:_____

Telephone Number:_____

Email:_____

Submit this form to the Hospital's Privacy Officer.

This form should be placed in the patient's medical record.

Community Hospital, LLC **HP Form 03**
TPG Hospital, LLC d/b/a Northwest Surgical Hospital

REVOCATION OF AUTHORIZATION TO DISCLOSE PROTECTED HEALTH INFORMATION

Patient's Name (print):_____

Patient's Date of Birth:_____

I no longer want Community Hospital, LLC or TPG Hospital, LLC d/b/a Northwest Surgical Hospital, as applicable (the "Hospital"), to continue to share protected health information about the patient identified above ("Patient") with the following individual or entity ("Recipient"):

Recipient's Name (print): _____

Address:_____

Telephone Number: _____

I understand if the Hospital has already disclosed the Patient's protected health information to the Recipient in reliance upon my prior authorization, this revocation will only prevent future disclosure.

This form must be signed by either the Patient or by the Patient's personal representative.

If this form is signed by the Patient's personal representative, please provide a copy of the document naming the personal representative and provide a description of the personal representative's authority to act on behalf of the Patient:

_____

_____

_____ Date:_____
Signature of Patient or Patient's Personal Representative

Current Contact Information for Patient or Personal Representative signing this form:

Name (print):_____

Address:_____

Telephone Number:_____

Email:_____

Submit this form to the Hospital's Privacy Officer.

This form should be placed in the patient's medical record.