Pulmonary Consultants, PLLC
Breathe easier. Sleep better. Live healthier.

POLICY: PRIVACY OF PROTECTED HEALTH INFORMATION

PURPOSE: Personnel affiliated with Pulmonary Consultants, PLLC ("PROVIDER") shall maintain the privacy of patients' health information consistent with the requirements of the Health Insurance Portability and Accountability Act and its implementing regulations, 45 CFR Part 164 ("HIPAA Rules"), and all other applicable state and federal laws.

APPLICATION

1. Protected Health Information. This policy applies to any information concerning a patient's physical or mental health, health care, or payment for health care that may identify or refer to the patient. It applies to any such information in any form, *e.g.*, oral, written, electronic, photographs, videos, *etc.* It applies to patient information about deceased patients if the patient has been dead less than 50 years. It applies to patient information that is created, received or maintained by PROVIDER, including information received from other healthcare providers. It does not apply to data from which all identifying information has been removed so that the information cannot be linked to a particular patient. (45 CFR § 160.103)

2. Access, Use or Disclosure. This policy applies to the internal access to or use of protected health information in addition to disclosure of such information to entities outside PROVIDER. (45 CFR §§ 160.103 and .502)

3. Personnel. This policy applies to all PROVIDER personnel, including administration, medical staff, clinical staff, office staff, volunteers, *etc.* It also applies to PROVIDER'S business associates who create, receive, maintain, or transmit protected health information on PROVIDER's behalf, including consultants, accountants, attorneys, IT specialists, vendors, health information organizations, *etc.* (45 CFR §§ 160.103 and .502)

4. Privacy Officer and Security Officer. PROVIDER shall designate in writing a Privacy Officer and Security Officer to facilitate and ensure compliance with relevant privacy and security regulations and policies. The Privacy Officer shall have primary responsibility for implementing and overseeing compliance with the requirements of the HIPAA privacy rules and these policies, and for responding to questions, complaints or other issues that arise concerning patient privacy. The Security Officer shall have primary responsibility for implementing and overseeing compliance with the requirements of the HIPAA security rules and associated policies as set forth in the following policies:

IS001	System Backup
IS003	Greenway EMR Security
IS006	Computer Security – Client Level
IS011	EMR Access for Research and Insurance Monitors
IS012	IT Disaster Recovery Plan
IS013	Data Storage Standards
IS014	Data Classification
IS015	IS Risk Management Assessment
IS016	Transmitting PHI Across the Internet
IS017	Wireless Network Access
IS018	Incident Management

The Privacy and Security Officers shall work together to update and implement policies as necessary to comply with applicable laws. (45 CFR § 164.530(a))

USE AND DISCLOSURE OF PROTECTED HEALTH INFORMATION

5. Compliance with Applicable Law. PROVIDER personnel shall maintain the privacy of PROVIDER's protected health information as required by:

a. The HIPAA Rules. This policy shall be interpreted and applied so as to comply with the requirements of the HIPAA privacy rules (45 CFR § 164.500 *et seq*.), security rules (45 CFR § 164.301 *et seq*.), and breach notification rules (45 CFR § 164.300 *et seq.*) as they shall be amended. The regulations, FAQs, and other helpful information concerning the HIPAA Rules are found at the Office of Civil Rights website, http://www.hhs.gov/ocr/privacy/index.html. PROVIDER personnel should be familiar with HIPAA rule requirements as described in these policies and should review the referenced regulations when responding to specific situations.

b. Notice of Privacy Practices. A copy of the Notice of Privacy Practices is incorporated into these policies. The Notice of Privacy Practices summarizes PROVIDER's privacy practices and policies. PROVIDER personnel are expected to know and comply with the operative Notice of Privacy Practices. (45 CFR § 164.520)

c. Other Laws. To the extent another federal or state law is more restrictive than HIPAA, PROVIDER personnel should comply with the more restrictive law. (45 CFR § 160.202 *et seq*.)

6. Use and Disclosure of Protected Health Information—No Authorization Needed. Unless PROVIDER has agreed to keep information confidential as provided in Section 17, below, PROVIDER personnel may generally use or disclose protected health information without the patient's or personal representative's written authorization (as described in Section 7, below) in the following circumstances. If you have questions about these circumstances, consult the Privacy Officer.

a. Treatment. PROVIDER personnel may use or disclose protected health information to treat the patient. For example, PROVIDER personnel may use or disclose information to evaluate the patient; to schedule appointments; to obtain information needed to treat the patient; make referrals; *etc.* In addition, PROVIDER personnel may disclose information to other health care providers so that the other providers may properly treat the patient. (45 CFR §§ 164.501 and .506)

b. Payment. PROVIDER personnel may use or disclose protected health information to obtain payment for services rendered to the patient. For example, PROVIDER personnel may contact third party payors to obtain pre-authorization or submit claims; perform billing functions; send a claim to collections; *etc.* PROVIDER personnel may also disclose protected health information to another provider so the other provider may obtain payment for his or her services. (45 CFR §§ 164.501 and .506)

c. Health Care Operations. PROVIDER personnel may use or disclose protected health information for PROVIDER's internal health care operations such as quality assurance, credentialing, peer review, training, legal services, business planning, customer services, etc. PROVIDER personnel may disclose certain protected health information for another provider's health care operations if (1) the other provider had a treatment relationship with the patient, and (2) the information is for the other provider's quality assurance, credentialing, peer review or similar purposes. PROVIDER personnel may not disclose protected health information to other providers for the other provider's other health care operations. (45 CFR §§ 164.501 and .506)

d. Personal Representatives. In the case of minors, deceased patients, or other patients who lack capacity to make their own healthcare decisions, PROVIDER personnel may disclose information to the parent, guardian, or other personal representative with authority to make health care decisions for the patient under applicable state law. PROVIDER personnel may decline to disclose

Kim C. Stanger
Phone (208) 383-3913
kcstanger@hollandhart.com
www.hollandhart.com

information to the personal representative if they believe it would not be in the patient's best interest to disclose the information. (45 CFR § 164.502(g))

e. To Family, Close Friends, or Others Involved in Care or Payment. PROVIDER personnel may disclose protected health information to family members, close friends, or others involved in the patient's healthcare or payment for healthcare under the following circumstances: (1) if the patient is present and has capacity, the patient either agrees to the disclosure or does not object despite having the opportunity to do so, and the practitioner reasonably believes that, under the circumstances, the patient does not object to disclosure; (2) if the patient is not present or the patient lacks capacity, but the practitioner believes that disclosure is in the patient's best interest; or (3) If the patient is deceased, and disclosure is not inconsistent with the patient's expressed wishes prior to his death. PROVIDER personnel should only disclose information relevant to the person's involvement in the patient's health care. (45 CFR § 164.510)

f. Facility Directory. Unless the patient asks to be a "do not publish", PROVIDER personnel may disclose the following information to a practitioner, visitor, or other person who asks for the patient by name: (1) the patient's name; (2) the patient's general condition; and (3) the patient's location in the facility. PROVIDER personnel may also disclose the patient's religious affiliation to clergy so long as the patient has not objected to such disclosures. (45 CFR § 164.510)

g. To Avert Serious Threat. PROVIDER personnel may disclose information if necessary to prevent or lessen serious and imminent harm to the patient or others. The disclosure may only be made to someone with the ability to avert the harm, *e.g.,* the police. (45 CFR § 164.512(j))

h. Disclosures Required by Law. PROVIDER personnel may disclose information to the extent another law requires disclosure (*e.g*., to report abuse, treatment of the victim of a crime or gunshot wounds, certain communicable diseases, threats to others, *etc*). Any disclosure should be limited to the extent required by that other law. This exception does not apply where another law merely allows, but does not require, disclosure. (45 CFR § 164.512(a), (c))

i. Subpoenas and Court Orders. PROVIDER personnel may disclose information pursuant to a court order, warrant, subpoena or administrative demand, but only if certain conditions are satisfied. PROVIDER personnel should immediately contact the Privacy Officer if they are presented with a court order, subpoena, or request from a lawyer or prosecutor. The Privacy Officer should review 45 CFR § 164.512(e) before responding to the order, warrant, subpoena or request. PROVIDER personnel should not disclose information orally if the order, warrant or subpoena only requires disclosure of records.

j. Workers Compensation. PROVIDER personnel may disclose information relevant to a workers compensation matter as authorized by and to the extent necessary to comply with laws relating to workers compensation claims. (45 CFR § 164.512(l))

k. Police, Regulators, and Other Government Officials. PROVIDER personnel may disclose information to the police or other government officials if certain conditions are satisfied. PROVIDER personnel should immediately contact the Privacy Officer if they receive requests from government officials. The Privacy Officer should review 45 CFR § 164.512(b), (c)-(g), and (k) before responding to such requests to ensure compliance with the regulations. Per Section 6(g), above, PROVIDER personnel may immediately contact the police if necessary to avert serious harm, to report a crime on the premises, or in response to a police request to identify a fugitive or victim.

l. Public Health Activities. PROVIDER personnel may disclosure limited information to proper authorities for certain public health activities, such as reporting births, deaths, certain diseases, etc. In addition, personnel may disclose information about immunizations to schools if state law conditions student enrollment on such information, and PROVIDER personnel obtain and document the student's or personal representative's consent to disclose the information. PROVIDER personnel should

Kim C. Stanger
Phone (208) 383-3913
kcstanger@hollandhart.com
www.hollandhart.com

review the requirements in 45 CFR § 164.512(b) or consult with the Privacy Officer to ensure such disclosures are made appropriately.

PROVIDER personnel should contact the Privacy Officer if they have questions or concerns about whether information should be accessed, used or disclosed without the patient's authorization.

7. Authorization for Use or Disclosure. Unless one of the foregoing exceptions apply, PROVIDER personnel must generally obtain written authorization from the patient or personal representative before using or disclosing protected health information internally or outside PROVIDER. The written authorization must contain certain information and statements required by 45 CFR § 164.508(c) to be valid. In addition, the authorization may not be combined with any other document. For these reasons, PROVIDER personnel should normally require and use PROVIDER's approved patient authorization form. Outside authorizations should be reviewed by the Privacy Officer or Administrator to confirm compliance. PROVIDER personnel should only disclose the information identified in the authorization to the persons identified in the authorization. Providers generally cannot condition treatment on provision of an authorization. PROVIDER personnel must retain a copy of the authorization. If the authorization is requested by someone other than the patient or the patient's personal representative, PROVIDER personnel must also give the patient or personal representative a copy of the authorization. (45 CFR § 164.508) Special rules apply to certain types of uses or disclosures as follows:

a. Psychotherapy Notes. Psychotherapy notes are notes recorded by a mental health professional documenting or analyzing the content of conversations during a private, group, joint or family counseling session and should be separated from the rest of the medical records. They do not include prescriptions, clinical test results, diagnosis, treatment plans, progress data, *etc.* The maker of psychotherapy notes may use them for his or her own treatment or training purposes, but any other uses or disclosures generally require the patient's written authorization. An authorization for psychotherapy notes may not be combined with any other authorization. (45 CFR §§ 164.501 and 164.508)

b. Marketing. PROVIDER personnel must obtain the patient's written authorization before using or disclosing protected health information for marketing purposes, *i.e.*, to make a communication about a product or service that encourages recipients to purchase or use the product. Written authorization is not required for the following marketing communications: (1) a face-to-face communication with patient; (2) a promotional gift of nominal value; and/or (3) communications for treatment purposes (*e.g.*, to recommend or direct alternative treatments or therapies) unless financial remuneration is received in exchange for making the communication. (45 CFR § 164.508) PROVIDER personnel should consult with the Privacy Officer before accepting remuneration or agreeing to make marketing communications in exchange for financial remuneration. If remuneration is received, the written authorization must state that remuneration is involved.

c. Sale of Information. The patient's written authorization is needed before PROVIDER personnel may disclose protected health information in exchange for remuneration. The authorization must state that the disclosure will result in remuneration to PROVIDER. (45 CFR §§ 164.502 and .508)

d. Fundraising. PROVIDER personnel may disclose limited patient information to a business associate or institutionally related foundation to help raise funds for PROVIDER if certain conditions are satisfied. All such requests for information or fundraising plans shall be reviewed by the Privacy Officer or *Administrator* to ensure compliance with applicable regulations, including 45 CFR § 164.512(f)) Recipients of fundraising communications have the right to opt out of receiving fundraising information.

e. Research. All requests to access, use or disclose protected health information shall be reviewed and addressed by the Privacy Officer. The Privacy Officer shall review appropriate HIPAA Rules concerning research prior to approving such requests, including 45 CFR §§ 164.508 and 164.512(i).

Kim C. Stanger
Phone (208) 383-3913
kcstanger@hollandhart.com
www.hollandhart.com

8. Minimum Necessary Standard. When using, disclosing or requesting protected health information, PROVIDER personnel must make reasonable efforts to limit information to the minimum necessary to accomplish the purpose of the use, disclosure, or request. (45 CFR §§ 164.502(b) and 164.514(d))

a. Routine Requests or Disclosure of Protected Health Information. The "minimum necessary standard" does not apply to disclosures to other health care providers for purposes of treating the patient. The minimum necessary standard generally applies to all other routine disclosures of information, including disclosures to third party payors to secure payment; disclosures to business associates; *etc*. PROVIDER personnel should not request the disclosure of the entire medical record unless they require the entire medical record for legitimate uses. Each Department shall establish protocols to limit the information routinely requested or disclosed to the amount necessary to achieve the purpose of the request or disclosure. (45 CFR § 164.514(d))

b. Non-Routine Requests or Disclosures of Protected Health Information. PROVIDER personnel shall review all non-routine requests or disclosures of protected health information on a case-by-case basis to limit the information requested or disclosed to the amount necessary to achieve the purpose of the request or disclosure. (45 CFR § 164.514(d))

c. Reliance on Person Requesting Information. If reasonable, PROVIDER personnel may rely on representations from the following persons that only the minimum necessary information is sought: public officials authorized to obtain information; requests by other providers or health plans; and requests by PROVIDER's professionals performing services for PROVIDER. (45 CFR § 164.514(d))

9. Access to Protected Health Information. PROVIDER personnel should only access protected health information if and to the extent necessary to perform their particular assigned job duties, as described below:

a. PROVIDER administration shall have access to any information as reasonably necessary to facilitate the effective and efficient operations of PROVIDER.

b. Medical staff, practitioners and other clinical personnel shall have access to any protected health information relevant to patients being treated, or who have been treated, by the practitioner or clinical personnel. They may also have access to information as necessary to engage in health care operations such as quality assurance, peer review or credentialing.

c. Billing personnel shall have access to any protected health information necessary to allow such personnel to bill for services rendered by PROVIDER, including financial information. Billing personnel should not normally access patients' medical records unless and to the extent necessary to properly bill for the service rendered.

d. Administrative support personnel (*e.g.*, receptionists, assistants, *etc*.) shall have access to only the protected health information that is reasonably necessary to allow the administrative personnel to fulfill their duties on behalf of PROVIDER. Administrative personnel should not normally access patients' medical records unless and to the extent necessary to allow them to properly fulfill their administrative duties.

e. Business associates of the PROVIDER who assist PROVIDER with administration, treatment, payment, and operations of the PROVIDER shall have access to protected health information that is reasonably necessary to allow the business associate to fulfill its duties on behalf of PROVIDER. PROVIDER must have a "business associate agreement" with business associates before the business associate may access protected health information as described below. Business associates' access shall be conditioned on and subject to the business associate agreement and the HIPAA Rules.

Kim C. Stanger
Phone (208) 383-3913
kcstanger@hollandhart.com
www.hollandhart.com

The unauthorized access of information outside the scope of such person's duties will subject the person to appropriate sanctions as provided below. (45 CFR § 164.514(d))

10. Verification. If PROVIDER personnel do not personally know the entity requesting protected health information, PROVIDER personnel shall take reasonable steps to verify the identity and authority of the entity before making the disclosure. (45 CFR § 164.514(h)) Reasonable steps may include asking for identification or credentials or asking questions that only the authorized person would know (*e.g.*, patient's birthdate, social security number, *etc.*)

11. Notice of Privacy Practices. As its name suggests, the Notice of Privacy Practices summarizes PROVIDER's privacy responsibilities and patients' rights. PROVIDER shall post a copy of its Notice in its reception area and on its website. PROVIDER personnel shall provide a copy of PROVIDER's Notice to the patient or personal representative no later than the first date of treatment.[1] If the first treatment is provided electronically, the Notice shall be sent contemporaneously to the patient by electronic means. PROVIDER personnel shall make a good faith effort to obtain the patient's or personal representative's written acknowledgment that they have received a copy of the Notice. If the patient or personal representative declines to sign the acknowledgement, PROVIDER personnel shall document in the patient's record their efforts to obtain the acknowledgement and why the acknowledgement was not obtained. The Notice shall be available for persons who would like to obtain a copy. The Privacy Officer shall be responsible for ensuring the Notice contains the elements required by 45 CFR § 164.520(b), and for updating the Notice to conform to PROVIDER's privacy practices or changes in the law. Changes in the Notice shall apply retroactively. PROVIDER personnel are responsible for knowing and complying with the Notice. (45 CFR § 164.520)

12. Logging Improper Disclosures. PROVIDER personnel shall log the following disclosures of protected health information: (1) disclosures that violate this policy or the HIPAA Rules; and (2) certain disclosures to government officials as described in Section 6(g)-(l), above. PROVIDER personnel are <u>not</u> required to log (1) disclosures for purposes of treatment, payment or health care operations; (2) disclosures to the patient or personal representative; (3) disclosures to family members or others involved in the care or payment for care; (4) disclosures pursuant to a written authorization; or (5) certain incidental disclosures. The disclosures shall be recorded on a log approved by the Privacy Officer, and shall include (1) the date of the disclosure; (2) name and address of the entity to whom disclosure is made; (3) (3) brief description of the information disclosed; and (4) the purpose of the disclosure. All improper disclosures must be reported to the Privacy Officer for review. The Privacy Officer should review the requirements in 45 CFR § 164.528 to confirm relevant requirements concerning the log. The log must be made available to the patient or personal representative if requested as described in Section 19, below. (45 CFR § 164.528)

13. Business Associates. PROVIDER personnel may disclose protected health information to PROVIDER's business associates who perform services on behalf of PROVIDER if (1) the information is needed for the services that the business associate performs on PROVIDER's behalf, and (2) if PROVIDER has a valid agreement with the business associate that complies with the requirements in 45 CFR §§ 164.314 and 164.504(e). PROVIDER personnel shall notify the Privacy Officer when they engage a business associate to provide services involving protected health information. The Privacy Officer shall ensure valid business associate agreements are in place before protected health information is disclosed to the business associate. Business associates shall cooperate with PROVIDER in responding to patient requests concerning their information as described in Sections 14-19, below. If PROVIDER personnel discover that a business associate has violated the HIPAA Rules or the business associate agreement, they shall immediately notify the Privacy Officer. The business associate

[1] This requirement applies to providers with a direct treatment relationship to the patient. Indirect treatment providers (*e.g.*, radiologists or pathologists) need only provide the Notice if requested by the patient. (45 CFR § 164.520(c)(2))

Kim C. Stanger
Phone (208) 383-3913
kcstanger@hollandhart.com
www.hollandhart.com

agreement shall set forth more fully PROVIDER's rights and obligations with regard to business associates. (45 CFR §§ 164.314, 164.502(e) and 164.504(e))

PATIENT RIGHTS CONCERNING THEIR HEALTH INFORMATION

14. Patients' Rights Concerning Their Protected Health Information. Patients or their authorized personal representatives have certain rights concerning the patient's protected health information as described below and in the Notice of Privacy Practices. To exercise these rights, the patient or personal representative should submit a written request to the Privacy Officer.

15. Patient Access to Information. The patient or their personal representative generally has a right to inspect and obtain a copy of protected health information in their "designated record set", *i.e*., their medical records and billing information. This includes medical records that PROVIDER has received from other providers, and any patient information maintained by business associates. To access or obtain copies of records, patients should submit a written request to the Privacy Officer identifying the records sought. PROVIDER personnel should discuss the scope of any request with the patient to ensure that the requested records are properly identified. The Privacy Officer should review the requirements in 45 CFR § 164.524 before responding. PROVIDER generally has 30 days to respond to a request. (45 CFR § 164.524(c))

a. Approval of Request. If the request to access information is approved, PROVIDER personnel should produce the information in the format requested (including the electronic format requested by the patient) if readily producible. If the patient agrees, PROVIDER personnel may provide a summary of the information. PROVIDER may charge a reasonable cost-based fee for providing the records, which costs include labor for copying, supplies for the copy, postage, and preparing the summary of the records. If the patient requests that an electronic copy of the records be sent elsewhere, PROVIDER personnel should generally agree if PROVIDER is reasonably able to send the information.

b. Denial of Request. PROVIDER may deny a patient's or personal representative's request under limited circumstances, *e.g*., if the patient seeks information outside their designated record set; psychotherapy notes; information prepared for legal proceedings; information that was provided under a promise of confidentiality; or if disclosure may result in substantial harm to the patient or others. Only the Privacy Officer may deny the patient's request to access information. The Privacy Officer should review the requirements in 45 CFR § 164.524 before denying the request. If the Privacy Officer denies the request, the Privacy Officer must advise the patient of the basis for the denial in writing. (45 CFR § 164.524(d))

c. Employee Records. This Section applies to PROVIDER personnel who have received treatment at PROVIDER. Such personnel are not permitted to access their own medical records; instead, they must request access pursuant to this Section.

16. Patient's Amendment of Health Records. The patient or personal representative may request that the patient's protected health information be amended by submitting a written request to the Privacy Officer. The request must explain the basis for the request. The Privacy Officer is responsible for reviewing and coordinating any response to a request for amendment. PROVIDER generally has 60 days to respond to a request. As necessary, the Privacy Officer shall consult with the relevant practitioner before agreeing to an amendment. (45 CFR § 164.526)

a. Approval of Amendment. If the Privacy Officer approves the amendment, the record should be amended consistent with PROVIDER's policy for amending or supplementing medical records. Any amendment becomes a part of the record. If other providers may have relied on an incorrect record, the Privacy Officer shall request permission from the patient to notify the other providers of the amendment. (45 CFR § 164.526(c))

Kim C. Stanger
Phone (208) 383-3913
kcstanger@hollandhart.com
www.hollandhart.com

b. Denial of Amendment. PROVIDER may deny the request if it did not create the record unless the originator is no longer available; if the patient did not have a right to access the record; or if the PROVIDER determines that the record is accurate and complete. The Privacy Officer should review the requirements in 45 CFR § 164.526 before denying a requested amendment. If the requested amendment is denied, the Privacy Officer will notify the patient or personal representative of the basis for the denial in writing. The patient or personal representative has the right to submit a statement disagreeing with the PROVIDER's decision and to have the statement attached to the record. (45 CFR § 164.526(d))

c. Notice of Amendment. If PROVIDER personnel receive notice of an amendment from another healthcare provider, they shall notify the Privacy Officer. The Privacy Officer shall ensure the relevant record is amended per 45 CFR § 164.526(e).

17. Patient's Request to Restrict Use or Disclosure of Information. Patients or personal representatives sometimes request restrictions on the use or disclosure of protected health information for purposes of treatment, payment or health care operations (*e.g.*, disclosures to other providers, insurers, *etc.*). Except for the situation described in Section 17(a), below, PROVIDER is not required to and generally does not agree to such restrictions because of the effect such restrictions have on internal operations and potential for liability. PROVIDER personnel should explain to the patient that PROVIDER's policy is not to agree to such restrictions. If the patient insists on the restriction, PROVIDER personnel should direct the patient to the Privacy Officer. Only the Privacy Officer may agree to restrictions on uses or disclosures for treatment, payment or health care operations. (45 CFR § 164.522(a))

a. Exception: Disclosure to Insurer. PROVIDER must limit disclosures to a health insurer if: (1) a health insurer requests information about an item or service; (2) the patient or another person on the patient's behalf paid for the entire item or service for which information is requested; and (3) the patient requests that the information not be disclosed to the insurer. If PROVIDER personnel receive such a request from the patient or personal representative, they should immediately direct the request to the Privacy Officer. The Privacy Officer shall review the request and payment information to confirm that a restriction on disclosure is required. If it is required, the Privacy Officer shall work with appropriate departments to ensure that the information is protected from disclosure to the health insurer as required by 45 CFR § 164.522(a)(1)(vi). If the restriction is not required, the Privacy Officer shall notify the patient.

b. Approval of Other Restrictions. If the Privacy Officer agrees to a different restriction on the use or disclosure of information for purposes of treatment, payment or healthcare operations, the Privacy Officer shall ensure that an appropriate notation is made in the medical record and take such additional action as required to accomplish the restriction. PROVIDER personnel shall comply with the restriction unless an emergency or legal requirement prevents the PROVIDER from complying with the restriction, or until the restriction is terminated. (45 CFR § 164.522(a))

18. Patient's Request to Communicate By Alternative Means. Patients or personal representatives may request that the PROVIDER communicate with them by alternative means (*e.g.*, by e-mail, by phone, by sealed envelope without a return address, *etc.*) or at alternative locations (*e.g.*, send all information to work or a different address). Patients should submit such requests in writing to the Privacy Officer. PROVIDER personnel may not ask the patient to explain the reason for the request. PROVIDER will accommodate all reasonable requests. (45 CFR § 164.522(b))

19. Patient's Request for Accounting of Certain Disclosures. The patient or personal representative may receive an accounting of certain disclosures of the patient's information by PROVIDER or PROVIDER's business associates. Such disclosures are tracked in the Accounting Log described in Section 12, above. The patient should submit the request for an accounting in writing to the Privacy Officer. The Privacy Officer shall coordinate the response to any request for accounting, including obtaining information about disclosures from PROVIDER's business associates. PROVIDER generally has 60 days to respond to the request. The patient or personal representative may receive the

Kim C. Stanger
Phone (208) 383-3913
kcstanger@hollandhart.com
www.hollandhart.com

first accounting within a 12-month period free of charge; after that, PROVIDER may charge a reasonable cost-based fee for all subsequent requests during that 12-month period. (45 CFR § 164.528)

ADMINISTRATIVE REQUIREMENTS

20. Training Workforce Members. The Privacy Officer shall ensure that all members of PROVIDER's workforce are trained concerning their privacy obligations, including officers, employees, contractors, and volunteers. New workforce members shall be trained as part of their initial orientation or within a reasonable time after undertaking services on behalf of PROVIDER. Workforce members shall generally be required to execute a confidentiality agreement. Each PROVIDER department shall provide periodic retraining concerning privacy issues as appropriate to the department, including training in response to privacy incidents or material changes in PROVIDER's privacy policies. Participation in training shall be documented and sent to the Privacy Officer or human resources department. (45 CFR § 164.530(b))

21. Safeguards and Security. Consistent with the requirements of the HIPAA privacy and security rules, PROVIDER personnel shall use reasonable physical, technical and administrative safeguards to protect participants' protected health information. (45 CFR §§ 164.301 *et seq*. and 164.530(c)) For example:

a. PROVIDER personnel should avoid leaving patient records or other information in open areas where unauthorized persons may see or access the information.

b. Computer screens containing other patient's information should be out of view of the patient, and the user should log out of screens showing patient information when the screen is unattended.

c. PROVIDER personnel should avoid discussing patient information in areas where others may overhear.

d. PROVIDER personnel should take reasonable steps to ensure that letters, faxes, e-mails, and other communications are sent to and received by the correct party, *e.g*., by confirming or checking the applicable number or address before sending the information, and by using appropriate cover sheets or privacy warnings.

e. PROVIDER may require employees, janitors, vendors, volunteers and others to execute confidentiality agreements.

f. PROVIDER personnel should secure computers, smart phones, PDAs, and patient records, and avoid creating situations in which unauthorized persons would be able to access computers, records, *etc.* Additional safeguards for electronic protected health information are described in the following policies

IS001	System Backup
IS003	Greenway EMR Security
IS006	Computer Security – Client Level
IS011	EMR Access for Research and Insurance Monitors
IS012	IT Disaster Recovery Plan
IS013	Data Storage Standards
IS014	Data Classification
IS015	IS Risk Management Assessment
IS016	Transmitting PHI Across the Internet
IS017	Wireless Network Access
IS018	Incident Management

Kim C. Stanger
Phone (208) 383-3913
kcstanger@hollandhart.com
www.hollandhart.com

Notwithstanding the foregoing, PROVIDER personnel are only required to utilize safeguards that are reasonable under the circumstances. PROVIDER personnel should use good judgment to ensure that privacy concerns do not interfere with effective patient care. Disclosures that are incidental to a permitted use do not violate this policy or the HIPAA Rules if PROVIDER personnel used reasonable safeguards to protect against such disclosures. (45 CFR § 164.502)

RESPONDING TO PRIVACY INCIDENTS

22. Reporting and Responding to Privacy Breaches. It is critical that suspected privacy violations are addressed and reported immediately to remedy or mitigate injury to the patient and penalties against those involved. PROVIDER personnel who become aware of a privacy breach should immediately take appropriate action to remedy or mitigate the breach (*e.g.*, by requesting the return of information; confirming that no additional disclosures have been or will be made; *etc.*). In addition, PROVIDER personnel shall immediately report suspected privacy violations to the Privacy Officer. The Privacy Officer shall promptly investigate and respond to any alleged privacy violation, and shall coordinate any efforts to address a confirmed privacy violation. To avoid HIPAA penalties, all privacy violations must be corrected and the correction documented within 30 days of the time that the violation was first discovered by PROVIDER personnel; accordingly, it is extremely important that PROVIDER personnel immediately report privacy violations. Failure to promptly report suspected privacy violations may result in sanctions described below. (45 CFR § 164.530(d))

23. Complaints. Patients and others may complain of suspected privacy violations. PROVIDER personnel should direct all complaints to the Privacy Officer. The Privacy Officer shall immediately take appropriate steps to investigate, mitigate, and respond to any complaint. The Privacy Officer shall document all complaints and the response to the complaints. (45 CFR § 164.530(f))

24. Notice of Privacy Breaches to Patient and HHS. PROVIDER may be required to notify the patient, HHS, and in some cases, local media if unsecured protected health information is disclosed in violation of the HIPAA Rules unless there is a low probability that the information has been compromised. The Privacy Officer shall review all suspected privacy violations to determine if notice is required by the rules. The Privacy Officer shall make all required notices of privacy breaches on behalf of PROVIDER. The process for evaluating and giving notice is addressed in Policy ___, Privacy Breach Notification. (45 CFR § 164.400 *et seq*.)

25. Sanctions for Violation. PROVIDER personnel who violate the provisions of these policies or applicable law (including the failure to timely report privacy violations) shall be subject to discipline as the circumstances warrant, which may include but is not limited to any of the following: warning, reprimand, suspension with or without pay, additional training, and/or termination of employment or contract. The Privacy Officer shall document sanctions imposed upon PROVIDER personnel in personnel files. (45 CFR § 164.530(e))

26. Non-Retaliation. PROVIDER personnel shall not intimidate or retaliate against any other PROVIDER personnel or patient for exercising any of the privacy rights granted by law. PROVIDER personnel shall not require a waiver of rights as a condition of treatment or payment. (45 CFR § 164.530(g))

DOCUMENTATION

27. Documentation. The Privacy Officer shall maintain copies of documents required by these policies and the HIPAA privacy and security rules for a period of six years from the later of when the document was created or the last effective date of the document. Such documents include, but are not limited to: these policies; authorizations for disclosure; the Notice of Privacy Practices; designation of Privacy and Security Officers; business associate contracts; privacy complaints and dispositions; workforce training; workforce sanctions; accounting logs; patient requests for access, accounting, or

Kim C. Stanger
Phone (208) 383-3913
kcstanger@hollandhart.com
www.hollandhart.com

amendments and PROVIDER's response; agreements to place restrictions on use or disclosure of information; *etc*. Such documentation may be maintained in electronic form. (45 CFR § 164.530(i))

28. **Questions.** Any questions or concerns about this policy or implementation of this policy should be directed to the Privacy Officer.

REFERENCES

HIPAA Privacy Rules, 45 CFR § 164.501 *et seq*.

HIPAA Breach Notification Rules, 45 CFR § 164.401 *et seq*.

HIPAA Security Rules, 45 CFR § 164.301 *et seq*.

Office of Civil Rights, http://www.hhs.gov/ocr/privacy/

RELATED DOCUMENTS AND POLICIES

Security of Electronic Protected Health Information, Policy No. _____

Privacy Breach Notification Policy, Policy No. _____

Notice of Privacy Practices

Accounting of Disclosure Log

Business Associate Agreement

Authorization for Disclosure of Protected Health Information

Kim C. Stanger
Phone (208) 383-3913
kcstanger@hollandhart.com
www.hollandhart.com