NOTE: *This sample policy is drafted to comply with the HIPAA breach notification rules as amended January 2013. The user should review applicable laws and regulations and modify this sample policy as appropriate to fit the user's circumstances and any additional requirements in state and federal laws, including state laws that may require reporting of computer security breaches that may result in identity theft.*

POLICY NAME: NOTICE OF PRIVACY BREACHES

PURPOSE: To enable _____ ("PROVIDER") to comply with applicable state and federal laws and regulations governing notice to affected persons in the event of a breach of patient privacy.

POLICY: PROVIDER personnel will maintain the privacy and security of patients' protected health information consistent with PROVIDER policies and applicable laws and regulations. PROVIDER will notify the patient, HHS, and in some cases, local media if there is a breach of unsecured protected health information unless PROVIDER can demonstrate a low probability that the information has been compromised.

APPLICATION.

1. PROVIDER Personnel. This Policy applies to all PROVIDER personnel, including PROVIDER administration, medical staff, clinical and administrative personnel, volunteers, and PROVIDER's business associates.

2. Breaches of Protected Health Information. This Policy applies only if there is a breach of a patient's individually identifiable health information. For purposes of this Policy, a breach is presumed if there is an unauthorized access, acquisition, use or disclosure of unsecured protected health information unless (1) PROVIDER can demonstrate that there is a low probability that the information was compromised based a risk assessment of certain factors described below, or (2) the situation fits within one of the following exceptions to the breach notification rule:

a. Any unintentional acquisition, access or use of protected health information by a member of PROVIDER's workforce or a person acting under PROVIDER's authority 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 violation of the HIPAA privacy rules.

b. Any inadvertent disclosure by a person who is authorized to access protected health information at PROVIDER to another person authorized to access patient information at PROVIDER and the patient information disclosed is not further used or disclosed in violation of the HIPAA privacy rules.

c. A disclosure of protected health information if PROVIDER has a good faith belief that the person to whom the disclosure was made would not reasonably have been able to retain such information.

d. The use or disclosure involves protected health information that has been "secured" according to standards published by HHS. Currently, this only applies to electronic patient information that has been properly encrypted consistent with standards published by HHS. HHS will publish future guidance for securing patient information on its website, www.hhs.gov/ocr/privacy/.
(45 CFR § 164.402).

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

PROCEDURE

1. Mitigating Potential Breaches. If PROVIDER personnel improperly access, acquire, use or disclose protected health information and immediate action may cure or mitigate the effects of such use or disclosure, PROVIDER personnel should take such action. For example, if PROVIDER personnel improperly access or acquire protected health information, they should immediately stop, close, and/or return the information. If PROVIDER personnel mistakenly disclose protected health information to the wrong person, they should immediately request the return of the information and confirm that no further improper disclosures will be made. If the potential breach is significant or requires further action to mitigate its effects, PROVIDER personnel should immediately contact their supervisor or the Privacy Officer for assistance and direction.

2. Reporting Potential Breaches to PRIVACY OFFICER. PROVIDER personnel shall immediately report any suspected breach of protected health information in violation of the HIPAA Rules or PROVIDER's privacy policies to the Privacy Officer. Failure to timely report suspected breaches may result in sanctions as described below.

3. Investigating Potential Breaches. The Privacy Officer shall promptly investigate any reported privacy breach or related patient complaint to determine whether there has been a "breach" of protected health information as defined above, and if so, how notice should be given. To determine whether a breach has occurred, Privacy Officer shall consider:

a. *Whether the alleged breach involved protected health information*, *i.e*., individually identifiable information concerning a patient's health, health care, or payment for health care, including financial or account information. (45 CFR § 164.402)

b. *Whether the alleged breach violates the HIPAA privacy rule.* Disclosures that are incidental to an otherwise permissible use or disclosure (*e.g.*, a patient overhears a physician speaking with another patient, or sees information about another patient on a whiteboard or sign-in sheet) do not violate the privacy rule so long as PROVIDER implemented reasonable safeguards to avoid improper disclosures. (45 CFR § 164.502)

c. *Whether there is a low probability that the protected health information has been compromised* considering relevant factors, including at least the following: (1) the nature and extent of the information involved; (2) the unauthorized person who used or received the information; (3) whether the information was actually acquired or viewed; and (4) the extent to which the risk to the information has been mitigated. (45 CFR § 164.402)

d. *Whether the alleged breach fits within one of the exceptions* identified in Section 2(a)-(d), above. (45 CFR § 164.402)

The Privacy Officer shall document his or her investigation and conclusions, including facts relevant to the risk assessment. (45 CFR §§ 164.414 and 164.530)

4. Notice—In General. If the Privacy Officer determines that a breach of unsecured protected health information has occurred, the Privacy Officer shall notify the patient, HHS, and the media (if required) consistent with this Policy and the requirements of 45 CFR §§ 164.404- .408 *et seq*. Any notice provided pursuant to this Policy must be approved and directed by Privacy Officer and/or PROVIDER Administration. No other PROVIDER personnel are authorized to provide the notice required by this Policy unless expressly directed by the Privacy Officer and/or PROVIDER Administration.

5. Notice to Individuals. If a breach of protected health information has occurred, the Privacy Officer shall notify the affected patient(s) without unreasonable delay and in no case later than 60 days after the breach is discovered. The notice shall include to the extent possible: (1) a brief description of what happened (*e.g*., the date(s) of the breach and its discovery); (2) a description of the types of information affected (*e.g*., whether the breach involved names, social security numbers, birthdates, addresses, diagnoses, *etc*.); (3) steps that affected patients should take to protect themselves from

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

potential harm resulting from the breach; (4) a brief description of what PROVIDER is doing to investigate, mitigate, and protect against further harm or breaches; and (5) contact procedures for affected persons to ask questions and receive information, which shall include a toll-free telephone number, e-mail address, website, or postal address at which the person may obtain more information. The notice shall be written in plain language. (45 CFR § 164.404)

a. Notice by Mail or Email. Privacy Officer shall notify the patient by first class mail to the patient's last known address. If the patient agrees, the notice may be sent by e-mail. The notice may be sent by one or more mailings as information is available. (45 CFR § 164.404(d))

b. Substitute Notice. If PROVIDER lacks sufficient contact information to provide direct written notice by mail to the patient, the Privacy Officer must use a substitute form of notice reasonably calculated to reach the patient. (45 CFR § 164.404(d))

(1) Fewer than 10 affected patients. If there is insufficient contact information for fewer than 10 affected patients, Privacy Officer shall provide notice by telephone, e-mail, or other means. If Privacy Officer lacks sufficient information to provide any such substitute notice, Privacy Officer shall document same. (45 CFR § 164.404(d)(2)(i))

(2) 10 or more affected patients. If there is insufficient contact information for 10 or more affected patients, Privacy Officer shall do one of the following after consulting with PROVIDER Administration: (1) post a conspicuous notice on the home page of PROVIDER's website for 90 days with a hyperlink to the additional information required to be given to individuals as provided above; or (2) publish a conspicuous notice in major print or broadcast media in the area where affected patients reside. The notice must include a toll-free number that remains active for at least 90 days so individuals may call to learn whether their protected health information was breached. (45 CFR § 164.404(d)(2)(ii))

c. Immediate Notice. If Privacy Officer believes that protected health information is subject to imminent misuse, Privacy Officer may provide immediate notice to the patient by telephone or other means. Such notice shall be in addition to the written notice described above. (45 CFR § 164.404(d)(3))

6. Deceased Patient; Notice to Next of Kin. If the patient is deceased and PROVIDER knows the address for the patient's next of kin or personal representative, the Privacy Officer shall mail the written notice described above to the next of kin or personal representative. If the PROVIDER does not know the address for the next of kin or personal representative, PROVIDER is not required to provide any notice to the next of kin or personal representative. The Privacy Officer shall document the lack of sufficient contact information. (45 CFR § 164.404(d)(1))

7. Notice to HHS. If the Privacy Officer determines that a breach of protected health information has occurred, the Privacy Officer shall also notify HHS of the breach as described below.

a. Fewer than 500 Affected Patients. If the breach involves the protected health information of fewer than 500 persons, the Privacy Officer may either (1) report the breach immediately to HHS as described in subsection (b), or (2) maintain a log of such breaches and submit the log to HHS annually within 60 days of the end of the calendar year. Instructions for maintaining and submitting the log are posted on the HHS website. (45 CFR § 164.408(c))

b. 500 or More Affected Patients. If the breach involves 500 or more persons, Privacy Officer shall notify HHS of the breach at the same time Privacy Officer notifies the patient or next of kin. Instructions for maintaining and submitting the log are posted on the HHS website. (45 CFR § 164.408(b))

8. Notice to Media. If a breach of protected health information involves more than 500 residents in a state, PROVIDER will also notify prominent media outlets in such state. The notice shall be provided without unreasonable delay but no later than 60 days after discovery of the breach. The notice shall contain the same elements of information as required for the notice to the patient described above. The

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

Privacy Officer shall work with PROVIDER Administration to develop an appropriate press release concerning the breach. (45 CFR § 164.406)

9. Notice from Business Associate. If PROVIDER's business associate discovers a breach of protected health information, the business associate shall immediately notify the Privacy Officer of the breach. The business associate shall, to the extent possible, identify each person whose information was breached and provide such other information as needed by PROVIDER to comply with this Policy. Unless the Privacy Officer directs otherwise, the Privacy Officer shall notify the patient, HHS, and, in appropriate cases, the media as described above. (45 CFR § 164.410)

10. Delay of Notice Per Law Enforcement's Request. The Privacy Officer shall delay notice to the patient, HHS, and the media if a law enforcement official states that the notice would impede a criminal investigation or threaten national security. If the officer's statement is in writing and specifies the time for which the delay is required, the Privacy Officer shall delay the notice for the required time. If the officer's statement is verbal, the Privacy Officer shall document the statement and the identity of the officer, and shall delay the notice for no more than 30 days from the date of the statement unless the officer provides a written statement confirming the need and time for delay. (45 CFR § 164.412)

11. Training Employees. PROVIDER shall train its workforce members concerning this Policy, including members' obligation to immediately report suspected privacy violations. The Privacy Officer shall ensure that this Policy is included in training given to new workforce members, and thereafter in periodic training as relevant to the work force members' job duties. (45 CFR § 164.530)

12. Sanctions. PROVIDER personnel may be sanctioned for a violation of this Policy, including but not limited to the failure to timely report a suspected privacy violation. PROVIDER may impose the sanctions it deems appropriate under the circumstances, including but not limited to termination of employment. (45 CFR § 164.530)

13. Documentation. The Privacy Officer shall prepare and maintain documentation required by this Policy for a period of six (6) years, including but not limited to reports or complaints of privacy violations; results of investigations, including facts and conclusions relating to the risk assessment; required notices; logs of privacy breaches to submit to HHS; sanctions imposed; *etc.* (45 CFR § 164.530)

14. Questions. Questions concerning this Policy should be directed to the Privacy Officer.

RELATED POLICIES

Policy No. ____, Privacy of Protected Health Information

Policy No. ____, Security of Electronic Protected Health Information

REFERENCES

HIPAA Breach Notification Rules, 45 CFR § 164.400 *et seq.*

HHS Commentary re Breach Notification Rules, 74 FR 42740 (Aug. 24, 2009) and 78 FR 5638 (Jan. 25, 2013)

HHS Guidance for Securing Protected Health Information, 74 FR 42741 (Aug. 24, 2009); also available at www.hhs.gov/ocr/privacy.

HIPAA Privacy Rules, 45 CFR § 164.500 *et seq.*

Idaho Identity Theft Statute, I.C. § 28-51-104 *et seq.*

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

Reviewed and approved by Governing Body:

_____
Representative of Governing Body

_____
Date

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