Status **Active** PolicyStat ID **6385074**

Origination	7/26/2018
Last Approved	3/12/2020
Effective	3/12/2020
Last Revised	3/12/2020
Next Review	6/30/2021
Owner	Lezah Cline: None
Area	Human Resources

HIPAA Privacy Rule

Policy Statement:

It is the policy of Scotland County Hospital to adhere to all Federal, State, and Local laws in the services and work practices it provides to all SCH employee, patients, vendors, contractors and family/ visitors.

The HIPAA Privacy Rule Policy is designed to educate and train all SCH employees to the standards of the Privacy Rule.

Definition:

Protected health information is personally identifiable health information held by a covered entity and protected under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule. Protected health information may only be disclosed for certain purposes. Examples of covered entities needing to transmit and process protected health information would include a health insurance company, a company sponsored health plan, or a doctor transmitting health information in electronic form to conduct financial and administrative transactions.

B**usiness associate** is a person or organization, other than a member of a covered entity's workforce, that performs certain functions or activities on behalf of, or provides certain services to, a covered entity that involve the use or disclosure of individually identifiable health information.

Business associate agreement (BAA)-In the BAA, a covered entity must impose specified written safeguards on the individually identifiable health information used or disclosed by its business associates.

Procedure:

The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other

personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. The Privacy Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The rule also gives patients' rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.

The HIPAA privacy Rule for the first time creates national standards to protect individuals' medical records and other personal health information.

- It gives patients more control over their health information.
- It sets boundaries on the use and release of health records.
- It establishes appropriate safeguards that healthcare providers and other must achieve to protect the privacy of health information.
- It holds violators accountable with civil and criminal penalties that can be imposed if they violate patients' privacy rights.
- And it strikes a balance when public responsibility supports disclosure of some forms of data, for example to protect public health.

Scotland County Hospital will provide the required HIPAA training for all SCH employees upon Hiring through the New Employee Orientation process and annually as mandated in the Educational Training Fair.

The HIPAA Privacy Rule Policy applies to many faucets of the SCH organization and the following procedures describes the protocol required for the enforcement of the Rule in reference to SCH.

Business Associates

Most health care providers and health plans do not carry out all of their health care activities and functions by themselves. Instead, they often use the services of a variety of other persons or businesses. The Privacy Rule allows covered providers and health plans to disclose protected health information to "business associates" if the providers or plans obtain satisfactory assurances that the business associate will use the information only for the purposes for which it was engaged by the covered entity, will safeguard the information from misuse, and will help the covered entity comply with some of the covered entity's duties under the Privacy Rule. In general, Business associate functions or activities on behalf of a covered entity include:

- Claims processing.
- Data analysis.
- Utilization review.
- Billing.

Business associate services to a covered entity are limited to legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services. Examples of business associates include:

- A third party administrator that assists a health plan with claims processing.
- A CPA firm whose accounting services to a health care provider involve access to protected health information.
- An attorney whose legal services to a health plan involve access to protected health information.
- A consultant that performs utilization reviews for a hospital.
- A health care clearinghouse that translates a claim from a nonstandard format into a standard transaction on behalf of a health care provider and forwards the processed transaction to a payer.
- An independent medical transcriptionist that provides transcription services to a physician.
- A pharmacy benefits manager that manages a health plan's pharmacist network.

When a covered entity uses a contractor or other non-workforce member to perform "business associate" services or activities, the Privacy Rule requires that the covered entity include certain protections for the information in a business associate agreement (BAA). Moreover, a covered entity may not contractually authorize its business associate to make any use or disclosure of protected health information that would violate the rule.

Covered entities may disclose protected health information to an entity in its role as a business associate only to help the covered entity carry out its health care functions — not for the business associates independent use or purposes, except as needed for the proper management and administration of the business associate.

When an employer sponsors a health plan having more than 49 participants or having administration services provided by an entity not part of the employer's own organization, business associate agreements (BAAs) must be maintained if the employer has access to protected health information.

Many employers are free from the obligation to establish and maintain BAAs because they do not maintain protected health information. If an employer-sponsored health plan provides benefits solely through an insurance contract with a health insurance carrier or health maintenance organization (HMO), such an employer would likely be exempt from maintaining HIPAA BAAs. The key to remaining exempt is for an employer to receive only enrollment information from employees and only summary claims history information from the carrier or HMO. If the employer maintains such a "hands-off" strategy towards handling protected health information, the carrier or HMO would likely be the covered entity under HIPAA.

The federal laws regarding BAAs are located at 45 CFR § 164.502(e), 29 CFR § 164.504(e), 45 CFR § 164.532(d), and 45 CFR § 164.532(e).

Important: Many states have enacted state privacy laws which are more stringent than federal HIPAA regulations; such state laws are not superseded by HIPAA. Employers should consult with legal counsel familiar with individual state regulations when developing a health privacy strategy. To illustrate the importance of this issue, consider that improper handling of a single health insurance enrollment form could be a violation of the law in the state of California (e.g, the Insurance Information and Privacy Protection Act, Insurance Code § 791 et seq., and the Information Practices Act, Civil Code § 1798 et seq). Therefore, even employers with a single employee should consider the impact of state laws related

to privacy.

Application to Health Plans

BAAs must be maintained by SCH as a sponsorof a self-funded health plan with more than 49 participants. HIPAA regulations generally apply to employers who sponsor self-funded medical, dental, or vision plans. Additionally, as a sponsor of a health flexible spending account (FSA) with medical reimbursement, services monitored and provided through the third party administrator must generally comply with these regulations even if their medical plan is fully insured through a carrier.

The U.S. Department of Health and Human Services published its Final Rule on HIPAA Privacy, Security, and Enforcement (also referred to as the HIPAA Privacy and Security Rules). The final rule includes updated BAA requirements.

Requirements

SCH may create a BAA with a business associate. A business associate may also create a BAA to subcontract with another business associate. Such an agreement must limit the business associate to use or disclose protected health information only as permitted or required by its business associate contract or as required by law. A business associate is directly liable under the HIPAA rules and subject to civil and, in some cases, criminal penalties for making uses and disclosures of protected health information that are not authorized by its contract or required by law. A business associate also is directly liable and subject to civil penalties for failing to safeguard electronic protected health information in accordance with the HIPAA Security Rule.

The following 10 requirements exist for any written BAA:

A. **Use.** Establish the permitted and required uses and disclosures of protected health information by the business associate.

B. **Limit.** Provide that the business associate will not use or further disclose the information other than as permitted or required by the contract or as required by law.

C. **Safeguard.** Require the business associate to implement appropriate safeguards to prevent unauthorized use or disclosure of the information, including implementing requirements of the HIPAA Security Rule with regard to electronic protected health information.

D. **Inform.** Require the business associate to report to the covered entity any use or disclosure of the information not provided for by its contract, including incidents that constitute breaches of unsecured protected health information.

E. **Report.** Require the business associate to disclose protected health information as specified in its contract to satisfy a covered entity's obligation with respect to individuals' requests for copies of their protected health information, as well as make available protected health information for amendments (and incorporate any amendments, if required) and accountings.

F. **Comply.** To the extent the business associate is to carry out a covered entity's obligation under the Privacy Rule, require the business associate to comply with the requirements applicable to the obligation.

G. **Account.** Require the business associate to make available to the U.S. Department of Health

and Human Services (HHS) its internal practices, books, and records relating to the use and disclosure of protected health information received from, or created or received by the business associate on behalf of, the covered entity for purposes of HHS determining the covered entity's compliance with the HIPAA Privacy Rule.

H. **Liquidate.** At termination of the contract, if feasible, require the business associate to return or destroy all protected health information received from, or created or received by the business associate on behalf of, the covered entity.

I. **Enforce.** Require the business associate to ensure that any subcontractors it may engage on its behalf that will have access to protected health information agree to the same restrictions and conditions that apply to the business associate with respect to such information.

J. **Terminate.** Authorize termination of the contract by the covered entity if the business associate violates a material term of the contract. Contracts between business associates and business associates that are subcontractors are subject to these same requirements.

Record-keeping Requirements

SCH will adopt reasonable and appropriate policies and procedures to comply with the provisions of the Security Rule. A covered entity must maintain, until six years after the later of the date of their creation or last effective date, written security policies and procedures and written records of required actions, activities, or assessments (45 C.F.R. § 164.316).

Enforcement

The U.S. Department of Health and Human Services Office for Civil Rights (OCR) is responsible for enforcing BAAs. However, other entities including the federal Department of Justice and the individual states' Attorneys General are authorized to seek enforcement action.

Penalties

SCH may be subject to a resolution agreement, which is a contract established with Missouri Department of Health and Senior Services.

SCH and any business associate are directly liable under the HIPAA Rules and subject to civil and, in some cases, criminal penalties for making uses and disclosures of protected health information that are not authorized by contract or required by law. The maximum civil penalty amounts are $50,000 for each violation up to a maximum of $1.5 million for identical provisions during a calendar year. Criminal penalties range from up to one year to up to 10 years for violations made for personal gain or malicious reasons.

SCH and any business associate may also be directly liable and subject to civil penalties for failing to safeguard electronic protected health information in accordance with the HIPAA Security Rule. Failures in this regard increase an employer plan sponsor's risk of exposure to litigation initiated by damaged participants or other interested parties.

Approval Signatures

Step Description	Approver	Date
CEO/Board	Dr Randy Tobler	3/12/2020
P&P Committee	Jasetia Buckallew	2/26/2020
Originating Authority	Cathie Overhulser	2/25/2020