Twin Falls County

Notice of Privacy Practices for Protected Health Information

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION PLEASE REVIEW IT CAREFULLY

Introduction	We understand your medical information is personal and we are committed to protecting your privacy as required by Federal and State Law. The *Standards for Privacy of Individually Identifiable Health Information* ("Privacy Rule") established a set of national standards for the protection of certain health information. The U.S. Department of Health and Human Services ("HHS") issued the Privacy Rule to implement the requirement of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). The Privacy Rule standards address the use and disclosure of individuals' health information - called "protected health information" by organizations subject to the Privacy Rule - called "covered entities", as well as standards for individuals' privacy rights to understand and control how their health information is used. 1. ***Personal Representatives.*** The Privacy Rule requires a covered entity to treat a "*personal representative*" the same as the individual, with respect to uses and disclosures of the individual's protected health information, as well as the individual's right under the Rule. 2. ***Special case: Minors.*** In most cases, parents are the personal representatives for their minor children. Therefore, in most cases, parents can exercise individual rights, such as access to the medial record, on behalf of their minor children. A major goal of the Privacy Rule is to assure that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well being.
Who is Covered by the Privacy Rule	**Health Plans.** Individual and group plans that provide or pay the cost of medical care are covered entities. Health plans include health, dental, vision, and prescription drug insurers, health maintenance organizations ("HMO's"), Medicare, Medicaid, Medicare+Choice and Medicare supplement insurers, and long-term care insurers. Health plans also include employer-sponsored group health plans, government and church-sponsored health plans, and multi-employer health plans. **Health Care Providers.** Every health care provider, regardless of size, who electronically transmits health information in connection with certain transactions, is a covered entity. **Health Care Clearinghouses.** *Health care clearinghouses* are entities that process nonstandard information they receive from another entity into a standard format or vice versa. **Business Associates.** In general, a business 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 Contract.** When a covered entity uses a contractor or other non-workforce member to perform *"business associate"* services or activities, the Rule requires that the covered entity include certain protections for the information in a business associate agreement (in certain circumstances governmental entities may use alternative means to achieve the same protections).

What Information is Protected	**Protected Health Information.** The Privacy Rule protects all "*individually identifiable health information*" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information "*protected health information (PHI)*". "*Individually identifiable health information*" is information, including demographic data, that relates to: ♦ the individual's past, present or future physical or mental health or condition, ♦ the provision of health care to the individual, or ♦ the past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual (e.g. name, address, birth date, Social Security Number). **De-Identified Health Information.** De-identified health information neither identifies nor provides a reasonable basis to identify an individual. There are not restrictions on the use of disclosure of de-identified health information.
General Principle for Uses and Disclosures	**Basic Principle.** A major purpose of the Privacy Rule is to define and limit the circumstances in which an individual's protected health information may be used or disclosed by covered entities. A covered entity may not use or disclose protected health information, except either: (1) as the Privacy Rule permits or requires; or (2) as the individual who is the subject of the information (or the individual's personal representative) authorizes in writing. **Required Disclosures.** A covered entity must disclose protected health information in only two situations: (1) to individuals (or their personal representatives) specifically when they request access to, or an accounting of disclosures of, their protected health information: and (2) to HHS when it is undertaking a compliance investigation or review or enforcement action.
Permitted Uses and Disclosures	**Permitted Uses and Disclosures.** A covered entity is permitted, but not required, to use and disclose protected health information, without an individual's authorization, for the following purposes or situations: 1. **To the individual**. A covered entity may disclose protected health information to the individual who is the subject of the information. 2. **Treatment, payment, health care operations.** A covered entity may use and disclose protected health information for its own treatment, payment and health care activities. ***Treatment*** is the provision, coordination, or management of health care and related services for an individual by one or more health care providers, including consultation between providers regarding a patient and referral of a patient by one provider to another. ***Payment*** encompasses activities of a health plan to obtain premiums, determine or fulfill responsibilities for coverage and provision of benefits, and furnish or obtain reimbursement for health care delivered to an individual and activities of a health care provider to obtain payment or be reimbursed for the provision of health care to an individual. ***Health care operations*** are any of the following activities: (1) quality assessment and improvement activities, including case management and care coordination; (2) competency assurance activities, including provider or health plan performance evaluation, credentialing, and accreditation; (3) conducting or arranging for medical reviews, audits, or legal services, including fraud and abuse detection and compliance

programs (4) specified insurance functions, such as underwriting, risk rating, and reinsuring risk; (5) business planning, development, management and administration; and (6) business management and general administrative activities of the entity, including but not limited to: de-identifying protected health information, creating a limited data set, and certain fundraising for the benefit of the covered entity.

3. **Uses and disclosures with opportunity to agree or object.** Informal permission may be obtained by asking the individual outright, or circumstances that clearly give the individual the opportunity to agree, acquiesce, or object.

   Facility directories. It is a common practice in many health care facilities, such as hospitals, to maintain a directory of patient contact information.

   For notification and other purposes. A covered entity also may rely on an individual's informal permission to disclose to the individual's family, relatives, or friends, or to other persons whom the individual identifies, protected health information directly relevant to that person's involvement in the individual's care or payment for care.

4. **Incidental use and disclosure.** The Privacy Rule does not require that every risk of an incidental use or disclosure of protected health information be eliminated (e.g., a hospital visitor may overhear a providers' confidential conversation with another provider for a patient, or may glimpse at patient information on paper or white board. The Privacy Rule permits certain incidental uses and disclosures of protected health information of occur when the covered entity has reasonable safeguards in place and minimum necessary policies and procedures to protect an individual privacy.

5. **Public interest and benefit activities.** The Privacy Rule permits use and disclosure of protected health information, without an individual's authorization or permission, for 12 national priority purposes.

   Required by law. Covered entities may use and disclose protected health information without individual authorization as required by law (including by statute, regulation, or court orders).

   Public health activities. Covered entities may disclose protected health information to (1) public health authorities authorized by law to collect or receive such information for preventing or controlling disease, injury or disability and to public health or other government authorities to receive reports of child abuse and neglect (2) entities subject to FDA regulation; (3) individuals who may have contracted or been exposed to a communicable disease when notification is authorized by law; and (4) employers, regarding employees, when requested by employers, for information concerning a work-related illness or injury.

   Victims of abuse, neglect or domestic violence. In certain circumstances, covered entities may disclose protected health information to appropriate government authorities regarding victims of abuse, neglect, or domestic violence.

Health oversight activities. Covered entities may disclose protected health information to health oversight agencies for purposes of legally authorized health oversight activities, such as audits and investigations necessary for oversight of the health care system and government benefit programs.

Judicial and administrative proceedings. Covered entities may disclose protected health information in a judicial or administrative proceeding if the request for the information is through an order from a court or administrative tribunal.

Law enforcement purposes. Covered entities may disclose protected health information to law enforcement officials for law enforcement purposes under the following six circumstances, and subject to specified conditions; (1) as required by law (including court orders, court-ordered warrants, subpoenas) and administrative requests; (2) to identify or locate a suspect, fugitive, material witness or missing person; (3) in response to a law enforcement official's request for information about a victim or suspected victim of a crime; (4) to alert law enforcement of a person's death, if the covered entity suspects that criminal activity caused the death; (5) when a covered entity believes that protected health information is evidence of a crime that occurred on its premises; and (6) by a covered health care provider in a medical emergency not occurring on its premises, when necessary to inform law enforcement about the commission and nature of a crime, the location of the crime or crime victims, and the perpetrator of the crime.

Decedents. Covered entities may disclose protected health information to funeral directors as needed, and to coroners or medical examiners to identify a deceased person, determine the cause of death, and perform other functions authorized by law.

Cadaveric organ, eye or tissue donation. Covered entities may use or disclose protected health information to facilitate the donation and transplantation of cadaveric organs, eyes and tissue.

Research. "Research" is any systematic investigation designed to develop or contribute to generalizable knowledge.

Serious threat to health or safety. Covered entities may disclose protected health information that they believe is necessary to prevent or lessen a serious and imminent threat to a person or the public, when such disclosure is made to someone they believe can prevent or lessen the threat (including the target of the threat).

Essential government functions. An authorization is not required to use or disclose protected health information for certain essential government functions (e.g., assuring proper execution of a military mission, conducting intelligence and national security activities that are authorized by law, providing protective services, making medical suitability determinations for U.S. State Department employees, protecting the health and safety of inmates or employees in a correctional institution, and determining eligibility for or conducting enrollment in certain government benefit programs).

	Worker's Compensation. Covered entities may disclose protected health information as authorized by, and to comply with, workers' compensation laws and other similar programs providing benefits for work-related injuries or illness. 6. **Limited data set.** A limited data set is protected health information from which certain specified direct identifiers of individuals and their relatives, household members, and employers have been removed.
Authorized Uses and Disclosures	**Authorization.** A covered entity must obtain the individual's written authorization for any use of disclosure of protected health information that is not for treatment, payment or health care operations of otherwise permitted or required by the Privacy Rule. A covered entity may not condition treatment, payment, enrollment, or benefits eligibility on an individual granting an authorization, except in limited circumstances. An authorization must be written in specific terms. It may allow use and disclosure of protected health information by the covered entity seeking the authorization, or by a third party. **Marketing.** Marketing is a communication about a product or service that encourages recipients to purchase or use the product or service. The Privacy Rule carves out the following health-related activities from this definition of marketing such as: ♦ Communications to describe health-related products or services, or payment for them, provided by or included in a benefit plan of the covered entity making the communication; ♦ Communications about participating providers in a provider or health plan network, replacement of or enhancements to a health plan, and health-related products or services available only to a health plan's enrollees that add value to, but are not part of, the benefit plan; ♦ Communications for treatment of the individual; and ♦ Communications for case management or care coordination for the individual, or to direct or recommend alternative treatments, therapies, health care providers, or care settings to the individual.
Limiting uses and Disclosures to the Minimum Necessary	**Minimum Necessary.** A central aspect of the Privacy Rule is the principle of "minimum necessary" use and disclosure. A covered entity must make reasonable efforts to use, disclose, and request only the minimum amount of protected health information needed to accomplish the intended purpose of the use, disclosure, or request. A covered entity must develop and implement policies and procedures to reasonably limit uses and disclosures to the minimum necessary. **Access and Uses.** For internal uses, a covered entity must develop and implement policies and procedures that restrict access and uses of protected health information based on the specific roles of the members of their workforce. These policies and procedures must identify the persons, or classes of persons, in the workforce who need access to protected health information to carry out their duties, the categories of protected health information to which access is needed, and any conditions under which they need the information to do their jobs.

	Disclosures and Requests for Disclosures. Covered entities must establish and implement policies and procedures for *routine, recurring disclosures, or requests for disclosures*, that limits the protected health information disclosed to that which is the minimum amount reasonably necessary to achieve the purpose of the disclosure. **Reasonable Reliance.** A covered entity may rely upon requests as being the minimum necessary protected health information from : (1) a public official, (2) a professional (such as an attorney or accountant) who is the covered entity's business associated, or (3) a researcher who provides the documentation or representation required by the Privacy Rule for research.
Notice and Other Individual Rights	**Privacy Practices Notice.** Each covered entity, with certain exceptions, must provide a notice of its privacy practices. The notice must state the covered entity's duties to protect privacy, provide a notice of privacy practices, and abide by the terms of the current notice. ***Notice distribution.*** A health plan must distribute its privacy practices notice to each of its enrollees by its Privacy Rule compliance date. Thereafter, the health plan must give its notice to each new enrollee at enrollment. ***Acknowledgement of Notice Receipt.*** A covered health care provider with a direct treatment relationship with individuals must make a good faith effort to obtain written acknowledgement from enrollees of receipt of the privacy practice notice. **Access.** Except in certain circumstances, individuals have the right to review and obtain a copy of their protected health information in a covered entity's designated record set. The "designated record set" is that group of records maintained by or for a covered entity that is used, in whole or part, to make decisions about individuals, or that is a provider's medical and billing records about individuals or a health plan's enrollment, payment, claims adjudication, and medical management record systems. **Amendment.** The Rule gives individuals the right to have covered entities amend their protected health information in a designated record set when that information is inaccurate or incomplete. **Disclosure Accounting.** Individuals have a right to an accounting of the disclosures of their protected health information by a covered entity or the covered entity's business associates. The Privacy Rule does not require accounting for disclosures: (1) for treatment, payment, or health care operations; (2) to the individual or the individual's personal representative; (3) for notification of or to persons involved in an individual's health care or payment for health care, for disaster relief, or for facility directories; (4) pursuant to an authorization; (5) of a limited data set; (6) for national security or intelligence purposes; (7) to correctional institutions or law enforcement officials for certain purposes regarding inmates or individuals in lawful custody; or (8)incident to otherwise permitted or required uses or disclosures.

Restriction Request. Individuals have the right to request that a covered entity restrict use or disclosure of protected health information for treatment, payment or health care operations, disclosure to persons involved in the individual's health care or payment for health care, or disclosure to notify family members or others about the individual's general condition, location, or death. A covered entity is under no obligation to agree to requests for restrictions.

Confidential Communications Requirements. Health plans and covered health care providers must permit individuals to request an alternative means or location for receiving communications of protected heath information by means other than those that the covered entity typically employs.

Health plans must accommodate reasonable requests if the individual indicates that the disclosure of all or part of the protected health information could endanger the individual. The health plan may not question the individual's statement of endangerment.

Privacy Policies and Procedures. A covered entity must develop and implement written privacy policies and procedures that are consistent with the Privacy Rule.

Privacy Personnel. A covered entity must designate a privacy official responsible for developing and implementing its privacy policies and procedures, and a contact person or contact office responsible for receiving complaints and providing individuals with information on the covered entity's privacy practices.

Mitigation. A covered entity must mitigate, to the extent practicable, any harmful effect it learns was caused by use or disclosure of protected health information by its workforce or its business associates in violation of its privacy policies and procedures of the Privacy Rule.

Data Safeguards. A covered entity must maintain reasonable and appropriate administrative, technical, and physical safeguards to prevent intentional or unintentional use or disclosure of protected health information in violation of the Privacy Rule and to limit its incidental use and disclosure pursuant to otherwise permitted or required use or disclosure.

Complaints. A covered entity must have procedures for individuals to complain about its compliance with its privacy policies and procedures and the Privacy Rule. The covered entity must explain those procedures in its privacy practices notice.

Retaliation and Waiver. A covered entity may not retaliate against a person for exercising rights provided by the Privacy Rule, for assisting in an investigation by HHS or another appropriate authority, or for opposing an act or practice that the person believes in good faith violates the Privacy Rule.

Fully-Insured Group Health Plan Exception. The only administrative obligations with which a fully-insured group health plan that has no more than enrollment data and summary health information is required to comply are the (1) ban on retaliatory acts and waiver of individual rights, and (2) documentation requirements with respect to plan documents if such documents are amended to provide for the disclosure of protected health information to the plan sponsor by a health insurance issuer or HMO that services the group health plan.

HIPAA Breach Notification Rule	This new HIPAA Breach Notification Rule only concerns the unauthorized acquisition, access, use or disclosure of unsecured patient health information as a result of a security breach. This Rule does not replace the existing HIPAA Privacy Rule that permits a covered entity to use and disclose patient health information, within certain limits and protections, for treatment, payment, and health care operations activities. The breach notification provisions are effective, and compliance is required for breaches occurring on or after September 23, 2009.
Breach Notification Requirements	**What constitutes a breach.** A breach is defined as the acquisition, access, use, or disclosure of unsecured protected health information which is not permitted by the HIPAA Privacy Rules and compromises the security or privacy of the protected health information. **What constitutes Unsecured Protected Health Information.** Unsecured protected health information is any patient health information that is not secured through a technology or methodology, specified by HHS, that renders the protected health information unusable, unreadable, or indecipherable to unauthorized individuals. **Exceptions to the Breach Notification Requirements.** The law identifies the following circumstances when a breach notification is NOT required: ♦ Any *unintentional* acquisition, access, or use of the protected health information by a workforce member (i.e., employees, volunteers, and other persons whose conduct is under the direct control of a covered entity, whether or not they are paid by the covered entity) or an individual, acting upon the authority of the HIPAA covered entity or a business associate who acquired, accessed, or used the protected health information in good faith and within the normal scope of his/her authority, and if that protected health information is not further used or disclosed. ♦ Any *inadvertent* disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity, business associate, or organized health care arrangement in which the covered entity participates, and the protected health information is not further used or disclosed in violation of the HIPAA Privacy Rules; ♦ A disclosure of protected health information where a covered entity or 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 (i.e., a laptop is lost or stolen and then recovered, and a forensic analysis of the computer shows that information was not opened, altered, transferred, or otherwise compromised); ♦ If law enforcement determines that notification would impede a criminal investigation or cause damage to national security, covered entities are allowed to delay notification, ***but only for up to 30 days as orally directed by the law enforcement agency, or for such longer period as the law enforcement agency specifies in writing***; and

	♦ Encryption and destruction are deemed as the technologies and methods for securing protected health information. Covered entities that have thus secured their protected health information through appropriate encryption or destruction methods are relieved of the notification obligation (unless otherwise required by federal or state law or necessary to mitigate the harmful effect of the breach). **Breach Notification.** HIPAA covered entities are required to notify the affected individuals of any unauthorized acquisition, access, use, or disclosure of unsecured protected health information without unreasonable delay but not later than 60 calendar days after discovery. Written notification should be sent via first class mail to each affected individual or personal representative at the last known address, unless the individual has indicated a preference for e-mail. In situations where it is deemed possible imminent misuse of unsecured protected health information, the entity may provide other forms of notice, such as by telephone or e-mail, in addition to the written notice.
How to File a Complaint	If you believe that a covered entity violated your (or someone else's) health information privacy rights or committed another violation of the Privacy Rule, you may file a complaint with the Office of Civil Rights (OCR). OCR can investigate complaints against covered entities. **Complaint requirements.** Your complaint must: 1. Be filed in writing, either on paper or electronically, by mail, fax, or e-mail; 2. Name the covered entity involved and describe the acts or omissions you believe violated the requirements of the Privacy Rule; and 3. Be filed within 180 days of when you knew that the act or omission complained of occurred. OCR may extend the 180-day period if you can show "good cause". **Anyone can file.** Anyone can file a complaint alleging a violation of the Privacy Rule. We recommend that you use the OCR Health Information Privacy Complaint Form Package. You can request a packet from an OCR regional office by e-mailing OCR at OCRMail@hhs.gov or see the payroll/benefits clerk. **HIPAA prohibits retaliation.** Under HIPAA an entity cannot retaliate against you for filing a complaint. You should notify OCR immediately in the event of any retaliatory action.

How to Submit your Complaint.

1. mail or fax your complaint to:

Office for Civil Rights, DHHS
2201 Sixth Avenue - Mail Stop RX-11
Seattle, Washington 98121
(206)615-2290; (206)615-2296 (TDD)
(206)615-2297 FAX

2. E-mail to OCRComplaint@hhs.gov

If you prefer, you may submit a ***written*** complaint in your own format. Be sure to include the following information:

- Your name
- Full address
- Telephone numbers
- E-mail address (if available)
- Name, full address and telephone number of the person, agency or organization you believe violated your (or someone else's) health information privacy rights were violated, or how the Privacy Rule otherwise was violated
- Any other relevant information
- Your signature and date of complaint

If you are filing a complaint on someone's behalf, also provide the name of the person on whose behalf your are filing.

The following information is ***optional***:

1. Do you need special accommodations for us to communicate with you about your complaint?
2. Who else can we call if we cannot reach you?
3. Have your filed your complaint somewhere else? If so, where?

Twin Falls County Social Services Privacy Contact:
If you have any questions about this Notice, or if you want to object to or complain about any use or disclosure or exercise any right as explained above, please call 208-736-4037 or email indigent@co.twin-falls.id.us.