PRIVACY NOTICE

The privacy provisions of HIPAA apply to health information created or maintained by health care providers who engage in certain electronic transactions, health plans, and health care clearinghouses. The Department of Health and Human Services (HHS) has issued the regulation, "Standards for Privacy of Individually Identifiable Health Information," applicable to entities covered by HIPAA. The Office for Civil Rights (OCR) is the Departmental component responsible for implementing and enforcing the privacy regulation.

This notice tells all employees what entities are covered by HIPAA, how and why personal information about employees will be collected, how it will be handled, and with whom the information is shared. We respect the privacy of personal information and maintain it securely. This notice applies to information regarding all current and former employees. Please review it carefully.

Covered Entities

Under the HIPAA Privacy Rule, Covered Entities and their business associates must guard against the misuse of an individual's identifiable health information and limit the sharing of such information. Covered Entities are:

- Medical service providers (hospitals, doctors, pharmacies, and laboratories)
- Medical Plans (via health insurance or self-insurance)
- Dental Plans (via health insurance or self-insurance)
- Vision Plans (via health insurance or self-insurance)
- Employee Assistance Plans that provide health benefits (via health insurance or self-insurance)
- Health insurance providers
- PPOs, HMOs, and managed health care organizations
- Health Care Spending or Reimbursement Accounts (flexible spending accounts under a cafeteria plan)
- Medical billing services

Business Associates

The HIPAA Privacy Rule also contains provisions regarding any third-party contractor or subcontractor that creates, maintains, or transmits protected health information on behalf of a covered entity. These persons or organizations, defined as "business associates" by the Privacy Rule, are bound by written business associate agreements to safeguard and limit the use and disclosure of protected health information. Business associates may include individuals or organizations performing one or more of the following functions or services for a covered entity: claims processing, data analysis, utilization review, billing, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services.

Why Personal Information is Collected

We will collect and use personal information:

- To determine eligibility for health care coverage
- To transmit premium payments to the health insurance carrier
- To provide test results to an officer of the company, government regulatory agencies, or companies that require certain tests under contract
- For pre-employment physicals and to determine fitness-for-duty of the employee's job.
- To evaluate work-related injuries and comply with workers' compensation laws.
- For requests for accommodation under the ADA
- To administer leave under FMLA (where applicable)
- To comply with OSHA, MSHA and similar state laws
- For judicial or administrative proceedings
- For the FBI and National Instant Criminal Background Check System (NICS) regarding mental health issues affecting gun possession

Personal Information Collected from Employees

We ask people seeking employment and benefits to provide certain information when they begin employment and enroll in a benefit plan. This information includes:

- Name, address, and phone number
- Social Security Number
- Birth Date
- Marital Status
- Information regarding current illnesses, injuries, or disabilities that may affect the ability to perform the job
- Consent to release all applicable information, including physical exam, drug screening, and fitness-for-duty results to the company and its agents and service providers

How We Protect Personal Information under Federal Law

Employee personal medical information is maintained in accordance with HIPAA, OSHA, the HITECH Act, the Genetic Information Nondiscrimination Act (GINA), and/or any other state or federal law to protect the privacy of such information. We will investigate and correct any alleged violation of privacy rules within 30 days of discovering the issue. Additionally, any qualifying third-party business associate that creates, maintains, or transmits PHI on behalf of our organization must strictly abide by the rules and restrictions set forth in their written business associate agreement.

How We Protect Personal Information under State Law

Employee personal medical information is maintained in accordance with our state law where such rules are more stringent than, but not contrary to, the federal law to protect the privacy of such information. In general, state laws that are contrary to HIPAA's privacy rule are preempted by the federal requirements, which mean that the federal requirements will apply. "Contrary" means that it would be impossible for a covered entity to comply with both the state and federal requirements, or that the provision of state law is an obstacle to accomplishing the full purposes and objectives of the Administrative Simplification provisions of HIPAA. The HIPAA privacy rule provides exceptions to the general rule of federal preemption for contrary state laws that (1) relate to the privacy of individually identifiable health information and provide greater privacy protections or privacy rights with respect to such information, (2) provide for the reporting of disease or injury, child abuse, birth, or death, or for public health surveillance, investigation, or intervention, or (3) require certain health plan reporting, such as for management or financial audits.

If a Security Breach Occurs

Upon receiving a report of a potential breach of protected health information, the company will follow the mandated breach notification procedures outlined in the HIPAA Security Rules.

Access to Your Protected Health Information (PHI)

You have the right of access to copy and/or inspect your PHI that we maintain in designated record sets. Certain requests for access to your PHI must be in writing, must state that you want access to your PHI and must be signed by you or your representative (e.g., requests for medical records provided to us directly from your health care provider). Access request forms are available upon request. We may charge you a fee for copying and postage.

Written Authorization

When applicable, an employee will need to complete a written authorization for the disclosure or restriction of protected health information. Additionally, protected health information will not be used or sold for marketing purposes without the written consent of affected parties.

Complaints

If you believe your privacy rights have been violated, you can file a complaint with us in writing. You may also file a complaint in writing with the Secretary of the U.S. Department of Health and Human Services in Washington, D.C., within 180 days of a violation of your rights. There will be no retaliation for filing a complaint.

For More Information

If you want more information on HIPAA as it applies to your personal health information or if you need to complete a written authorization or file a complaint, please contact:

- The company Owner or Human Resources department; or
- Customer Service for your plan's health insurance provider; or
- The U.S. Department of Health and Human Services, Office of Civil Rights, 200 Independence Avenue S.W., Washington, D.C. 20201. (877) 696-6775 (toll free): or
- Centers for Medicare and Medicaid Services, 7500 Security Blvd, Baltimore, MD 21244-1850. (877)-267-2323 (toll free).

Contact Information

Inquiries relating to any of the following should be directed to the individual listed below.

- Obtaining a copy of the health plan's Notice of Privacy Practices.
- Reporting a possible violation or infraction.
- Questions regarding uses and disclosures

Designated Contact:

_____ at _____

(HIPAA Compliance Officer or Plan Administrator) Phone Number

What is Protected Health Information (PHI)?

Under the HIPAA Privacy Rule, protected health information, or "PHI," refers to individually identifiable health information that can be transmitted in any form or medium by a covered entity or its business associate. Individually identifiable health information is that which can be linked to a particular person. Specifically, this information can relate 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.

Common identifiers of health information include names, social security numbers, addresses, and birth dates (see PRIVACY NOTICE on this poster).

What is Electronic Protected Health Information (ePHI)?

The HIPAA Security Rule applies to individual identifiable health information in electronic form or electronic protected health information, or "ePHI." It is intended to protect the confidentiality, integrity, and availability of ePHI when it is stored, maintained, or transmitted.

Uses & Disclosures of PHI

Covered entities must safeguard PHI by implementing policies and procedures to restrict access to and use of PHI. Furthermore, a covered entity must only use or disclose the minimum amount of PHI necessary. Required disclosures include:

- To an individual when requested & required by Section 164.524 (Access) & Section 164.528 (Accounting)
- To HHS, to investigate or determine compliance with Privacy Rule
- To the FBI and the National Instant Criminal Background Check System (NICS) for mental health issues regarding gun possession

Besides required disclosures, covered entities also may disclose PHI to their patients / health plan enrollees so that:

- Health plans can contact their enrollees, and
- Providers can talk to their patients

STATEMENT OF HIPAA PORTABILITY RIGHTS

Pre-existing condition certification no longer needed

After being amended by the Patient Protection and Affordable Care Act (PPACA), HIPAA offers new protections for workers and their families. The law provides additional opportunities to enroll in a group health plan if individuals lose other coverage or experience certain life events. HIPAA also prohibits discrimination against employees and their dependents based on any health factors they may have, including prior medical conditions, previous claims experience, and genetic information.

Under HIPAA, you and your family members cannot be denied eligibility or benefits based on certain health factors, including pre-existing condtions, when enrolling in a health plan. In addition, you may not be charged more than similarly situated individuals based on any health factors. The questions and answers below define the health factors and offer some examples of what is and is not permitted under the law.

Thus the pre-PPACA requirement for HIPAA certifications on pre-existing condition coverage is no longer required.

Right to get special enrollment in another plan

Under HIPAA, if you lose your group health plan coverage, you may be able to get into another group health plan for which you are eligible (such as a spouse's plan), even if the plan generally does not accept late enrollees, if you request enrollment within 30 days. (Additional special enrollment rights are triggered by marriage, birth, adoption, and placement for adoption.)

Therefore, once your coverage ends, if you are eligible for coverage in another plan (such as a spouse's plan), you should request special enrollment as soon as possible.

Prohibition against discrimination based on a health factor

Under HIPAA, a group health plan may not keep you (or your dependents) out of the plan based on anything related to your health. Also, a group health plan may not charge you (or your dependents) more for coverage, based on health, than the amount charged a similarly situated individual.

Right to individual health coverage

Under HIPAA, if you are an "eligible individual," you have a right to buy certain individual health policies (or in some states, to buy coverage through a high-risk pool) without a pre-existing condition exclusion. To be an eligible individual, you must meet the following requirements:

- You have had coverage for at least 18 months without a break in coverage of 63 days or more;
- Your most recent coverage was under a group health plan;
- Your group health coverage was not terminated because of fraud or nonpayment of premiums;
- You are not eligible for COBRA continuation coverage or you have exhausted your COBRA benefits (or continuation coverage under a similar state provision); and
- You are not eligible for another group health plan, Medicare, or Medicaid, and do not have any other health insurance coverage.

The right to buy individual coverage is the same whether you are laid off, fired, or quit your job. Therefore, if you are interested in obtaining individual coverage and you meet the other criteria to be an eligible individual, you should apply for this coverage as soon as possible to avoid losing your eligible individual status due to a 63-day break.

State flexibility

This certificate describes minimum HIPAA protections under federal law. States may require insurers and HMOs to provide additional protections to individuals in that state.

HIPAA AND THE DEFENSE OF MARRIAGE ACT (DOMA)

In *United States v. Windsor*, the Supreme Court held section 3 of the Defense of Marriage Act (DOMA) to be unconstitutional. Section 3 of DOMA had provided that federal law would recognize only opposite-sex marriages. **In light of the Windsor ruling, covered entities must consider the following regarding lawfully married same-sex spouses and same-sex marriage:**

1. At 45 CFR 160.103, the Privacy Rule includes the terms spouse and marriage in the definition of family member. Consistent with the Windsor decision, the term spouse includes individuals who are in a legally valid same-sex marriage. The term marriage includes both same-sex and opposite-sex marriages, and family member includes dependents of those marriages.

2. The definition of a family member is relevant to the application of §164.510(b), Standard Uses and Disclosures for Involvement in the Individual's Care and Notification Purposes, which permits covered entities to share protected health information (PHI) with a family member. Legally married same-sex spouses, regardless of where they live, are family members for the purposes of applying this provision.

3. The definition of a family member is also relevant to the application of §164.502(a)(5)(i), Use and Disclosure of Genetic Information for Underwriting Purposes. This provision prohibits health plans, other than issuers of long-term care policies, from using or disclosing genetic information for underwriting purposes. This includes the genetic tests of a same-sex spouse of the individual.

4. The Department of Health and Human Services (HHS) in 2016 issued its final rule on "Nondiscrimination in Health Programs and Activities" to expand discrimination protections under the Affordable Care Act and HIPAA. Individuals are now protected against discrimination in health care based on:

   - Race
   - Color
   - National Origin
   - Age
   - Disability
   - Sex and Gender Identity

MENTAL HEALTH INFORMATION FOR THE NICS

On January 4, 2016, the Department of Health and Human Services (HHS) modified the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule to expressly permit certain covered entities to disclose to the National Instant Criminal Background Check System (NICS) the identities of those individuals who, for mental health reasons, already are prohibited by Federal law from having a firearm.

The final rule gives states improved flexibility to ensure accurate but limited information is reported to the NICS. This rulemaking makes clear that, under the Privacy Rule, certain covered entities are permitted to disclose limited information to the NICS. The information that can be disclosed is the minimum necessary identifying information about individuals who have been involuntarily committed to a mental institution or otherwise have been determined by a lawful authority to be a danger to themselves or others or to lack the mental capacity to manage their own affairs.

The new modification is carefully and narrowly tailored to preserve the patient-provider relationship and ensure that individuals are not discouraged from seeking voluntary treatment. This rule applies only to a small subset of HIPAA covered entities that either make the mental health determinations that disqualify individuals from having a firearm or are designated by their states to report this information to NICS – and it allows such entities to report only limited identifying, non-clinical information to the NICS. The rule does not apply to most treating providers and does not allow reporting of diagnostic, clinical, or other mental health treatment information.

An individual who seeks help for mental health problems or receives mental health treatment is not automatically legally prohibited from having a firearm; nothing in this final rule changes that.

MOBILE DEVICES

Covered entities must comply with HIPAA Privacy and Security Rules to safeguard protected health information (PHI), even when using mobile devices. **Here are five steps we are taking to help safeguard PHI on mobile devices:**

1. Determine whether a mobile device will be used to access, receive, transmit, or store patients' health information.
2. Identify the risks when using mobile devices before transmitting any health information.
3. Create a mobile device risk management strategy, including privacy and security safeguards.
4. Develop, document, and implement safeguarding policies for mobile devices.
5. Conduct ongoing training for privacy and security awareness when using mobile devices.

BREACH NOTIFICATION

The Health Information Technology for Economic and Clinical Health Act (HITECH Act) requires HIPAA-covered entities and business associates to follow specific rules relating to the discovery of a breach of protected health information. These rules require covered entities and business associates to do the following when a security breach is discovered:

- Provide notification to affected individuals and to the Secretary of HHS following the discovery of a breach of unsecured protected health information.
- For a breach of unsecured protected health information involving more than 500 residents of a State or jurisdiction, provide notification to the media of breaches.
- In the case of a breach of unsecured protected health information at or by a business associate of a covered entity, the Act requires the business associate to notify the covered entity of the breach.

A "breach" is defined as the acquisition, access, use, or disclosure of protected health information in a manner which compromises its security or privacy.

A covered entity shall, following the discovery of a breach of unsecured protected health information, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of such breach.

The covered entity must send the required notification without unreasonable delay and in no case later than 60 calendar days after the date the breach was discovered.

ANTI-DISCRIMINATION NOTICE

General

A group health plan may not establish any rule for eligibility (including continued eligibility) of any individual to enroll for benefits under the terms of the plan that discriminates based on any health factor that relates to that individual or a dependent of that individual. This notice describes nondiscrimination rules that apply beginning the first day of the first plan year after July 1st, 2007.

Health Factors

The term "health factor" means, in relation to an individual, any of the following health status-related factors:

- Health status;
- Medical condition (including both physical and mental illnesses);
- Claims experience;
- Receipt of health care;
- Medical history;
- Genetic information;
- Evidence of insurability (including conditions arising out of acts of domestic violence or out of participations in recreational activities);
- Disability.

Eligibility Rules

Rules for eligibility include rules relating to any of the following:

- Enrollment;
- The effective date of coverage;
- Waiting (or affiliation) periods;
- Late and special enrollment;
- Eligibility for benefit packages;
- Benefits (including copayments and deductibles);
- Continued eligibility;
- Terminating coverage (including disenrollment) of any individual under the plan.

Nonconfinement and Actively-At-Work Provisions

A plan may not establish a rule for eligibility or set any individual's premium or contribution rate based on whether an individual is confined to a hospital or other health care institution or whether the individual is actively at work (including continuous employment).

Similarly-Situated Individuals

Distinctions among groups of similarly situated individuals may not be based on a health factor. Group health plans may limit or exclude coverage or benefits if the restriction is applied uniformly to all similarly situated individuals and is not directed at any individual participants or beneficiaries based on a health factor.

Exceptions for Wellness Programs

Special rules and exceptions apply to wellness programs (programs designed to promote health or prevent disease) that provide benefit incentives.

SECURITY NOTICE

For Employers Who Sponsor Health Benefit Plans for Employees

The confidentiality, integrity, and availability of any electronic protected health information (ePHI) collected or possessed by our organization (or our business associates) will be ensured via appropriate safeguards as specified under the HIPAA security rule. The security rule requires all covered entities to conduct a risk analysis and implement reasonable physical, technical, and administrative safeguards to prevent the unauthorized access, alteration, deletion, or transmission of ePHI.

Risk Analysis

This organization has conducted a risk analysis in compliance with the HIPAA security rule. This risk analysis included all of the following steps: collecting data on ePHI; identifying potential threats and vulnerabilities; assessing the likelihood and impact of potential threats; and documentation of relevant findings.

As per the Final HIPAA Omnibus Rule effective March 26, 2013, the following four factors must be considered in a risk analysis to determine whether the information was compromised:

1. To whom the information was impermissibly disclosed;
2. Whether the information was actually accessed or viewed;
3. The potential ability of the recipient to identify the subjects of the data; and
4. In cases where the recipient is the disclosing covered entity's business associate or is another covered entity, whether the recipient took appropriate mitigating action.

Safeguards

To ensure compliance with the HIPAA security rule, we have implemented a combination of physical, technical, and administrative safeguards to protect ePHI. Physical safeguards may include workstation and device security, technical safeguards may include access control and transmission security, and administrative safeguards may include designating a security official who is responsible for developing and implementing our security policies and procedures.

Policies, Procedures, and Documentation

Our HIPAA security rule compliance efforts are documented and may be readily available for review. This documentation includes some combination of the following:

- Risk management plan
- Risk analysis checklists
- Security violation monitoring reports
- Vulnerability scanning plans
- Lists of all user accounts with access to systems which store, transmit, or access ePHI
- Policies and procedures governing the use of virus protection software
- Data backup procedures
- Disaster recovery plans
- Inventory of all information systems to include network diagrams listing hardware and software used to store, transmit, or maintain ePHI
- Other documents specifically mandated or recommended by the HIPAA security rule