HIPAA Compliance

GATEWAYS COMMUNITY SERVICES

INFORMATION MANAGEMENT NEED TO KNOW

Definition: Need to know - the principle that states that a user should access only the specific information necessary to perform a particular function in the exercise of his/her appointed duties. Once access to an application is authorized, the authorized data user is still obligated to assess the appropriateness of each specific access on a need to know basis.

Following are examples where employees have a need to know individually identifiable information to complete their assigned job functions, as well as examples where employees do not have a need to know such information. These lists are intended to be examples only, and are not intended to be complete representations of situations where employees have a need to know individually identifiable information. Per the Gateways Community Services' policy, specific access to individually identifiable information is under the discretion of departmental director.

Examples of appropriate uses of individually identifiable information where employees have a need to know:

- Rendering direct care to specific consumers (including diagnosis, service agreement and assessment).
- Disease management and prevention activities such as immunization verification, screening for candidacy for specialized treatment programs or potential preventative interventions.
- At the request of the consumer. (Exception: Employee is not permitted access without a form signed by the consumer authorizing release of the information.)
- Administrative support activities including but not necessarily limited to appointment and scheduling coordination, complying with third party requirements, follow-up coordination, billing and collecting for services rendered to specific consumers, and maintenance of the record and/or information medium.
- Financial analysis to assess the business impact of consumer care, including but not limited to analysis of specific cases to assess impact of service/program redesign or in response to research requests (grants), and analysis of situations where it is necessary to join records from more than one system (for example, Vendor X and Vendor Y) together in order to analyze the full impact of that care.
- Performing reimbursement analysis on specific consumers.
- Performing activities in the course of development/fund raising, strategic planning, legal defense, or follow-up on a compliance complaint.
- Educational or teaching purposes or instructional requirement criteria (Interns).
- Performing quality assurance and/or regulatory compliance activities.
- Educational material or informational resources.
- Fund raising activities done at the request of an employee who has knowledge of the consumer or family's desire to donate to Gateways Community Services.

Examples specifically relevant:

- Administrative activities including enrollment, claims payment, coordination of benefits, customer service, SPEDIS reporting, data quality investigation, and quality improvement of administrative services.
- Utilization management activities for the purpose of assessing the appropriateness and efficiency of the services provided to a consumer member or group of consumer members, and for determining the contributing causes underlying certain financial results.
- Service coordination activities, including identification of members with a specific type or extent of health problems and provision of service coordination interventions.
- Grants.

Examples of inappropriate use of consumer identifiable information:

- Mass mailing fund raising solicitations to consumers with specific conditions, without the express approval of the consumer or guardian.
- Use of personal medical information in making employment decisions.
- Use of employee's personal medical information to see if the employee was really out sick, had a doctor's appointment, had a worker's compensation injury, etc.

Information Management Legally Restricted Information

Definition: Legally Restricted Information - individually identifiable information whose disclosure is specifically subject to additional legal requirements imposed by statute or administrative rule.

Examples of legally restricted information are:

- substance abuse treatment records
- sexual abuse treatment records
- mental health treatment records,
- certain diagnostic categories such as HIV/AIDS
- adolescent health information related to pregnancy, birth control, and/or sexually transmitted diseases.

NOTICE OF PRIVACY PRACTICES

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.

I. Introduction.

This Notice of Privacy Practices describes how we may use and disclose your protected health information to carry out treatment, payment or health care operations and for other purposes that are permitted or required by law. It also describes your rights to access and control your protected health information. "Protected health information" is information about you, including demographic information, that may identify you and that relates to your past, present or future physical or mental health or condition and related health care services.

II. Your Health Information Rights.
While the actual records that we maintain about you belong to us, the information contained in our records belongs to you. Under the federal Privacy Rules (42 CFR Part 160 and Part 164) you have the right to:

- Request a restriction on certain uses and disclosures of your information as provided by 45 CFR 164.522. Note, however, that we are not required to agree to a restriction that you may request. If we believe it is in your best interest to permit use and disclosure of your health information, we will notify you that your request for restriction will not be honored. If we agree to the requested restriction, we may not use or disclose your health information in violation of that restriction unless it is needed to provide emergency treatment.
- Obtain a paper copy of this Notice of Privacy Practices upon request
- Inspect and obtain a copy of your health record
- Amend your health record
- Obtain an accounting of certain disclosures of your health information
- Receive confidential communications of your health information by alternative means or at alternative locations
- revoke your authorization to use or disclose health information except to the extent that action has already been taken

lll. Our Responsibilities. This organization is required to:

- maintain the privacy of your health information
- provide you with a notice as to our legal duties and privacy practices with respect to information we collect and maintain about you
- abide by the terms of this notice
- notify you if we are unable to agree to a requested restriction
- accommodate reasonable requests you may have to communicate health information by alternative means or at alternative locations.

We reserve the right to change our practices and to make the new provisions effective for all protected health information we maintain. Should our information practices change, we will mail a revised notice to the address you've supplied us.

This notice was published on April 1, 2003 and becomes effective on April 14, 2003.

We will not use or disclose your health information without your authorization, except as described in this notice.

IV. Examples of How We Will Use or Disclose Your Protected Health Information.
Your protected health information may be used and disclosed by members of our staff and others outside of our office that are involved in your care and treatment for the purpose of providing services to you. Your protected health information may also be used and disclosed to enable us to be paid for the services we render to you.

Following are examples of the types of uses and disclosures of your protected health care information that we are permitted to make. These examples are not meant to be exhaustive, but to describe the types of uses and disclosures that may be made by our office.

Treatment:
We will use and disclose your protected health information to provide, coordinate, or manage your care, including your health care and any related services. This includes the coordination or management of your health care with a third party that has already obtained your permission to have access to your protected health information. For example, we would disclose your protected health information, as necessary, to service providers such as providers of early supports and services, or residential/day services, or physicians who may be treating you. Also, for example, we may use or disclose your protected health information, as necessary, to facilitate appointment or change of a guardian or other legal representative.

Payment:
Your protected health information will be used, as needed, to obtain payment for services that we provide to you. This may include certain activities that your health plan may undertake before it approves or pays for the services we recommend for you. For example, some health plans must make a determination that you are eligible for reimbursement for particular services before we can provide them to you and we must provide them with protected health information to enable them to make such a determination.

Healthcare Operations:
We may use or disclose, as-needed, your protected health information in order to support our own business activities. These activities include, but are not limited to, quality assessment activities, training and supervision of staff members, licensing, certification and conducting or arranging for other business activities. We may also disclose your protected health information to the NH Department of Health and Human Services or other agencies of the State of New Hampshire to comply with our contract with the State of New Hampshire and, if applicable, to determine your eligibility for publicly funded services.

We will share your protected health information with third party "business associates" that perform various activities that are essential to the operations of our organization. Whenever we have an arrangement between our organization and a business associate, we will limit the amount of protected health information that we provide to the minimum necessary to accomplish the particular task and we will have a written contract that contains terms that will protect the privacy of your protected health information.

We may use or disclose your protected health information, as necessary, to provide you with appointment reminders or information about treatment alternatives or other health-related benefits and services that may be of interest to you.

We may also use your health information to contact you in connection with limited marketing or fundraising communications for our agency that are permitted under the federal privacy rules. Any fundraising communication addressed to you will contain instructions describing how you may opt out of receiving such communications in the future.

V. Uses and Disclosures That We May Make Unless You Object.
In the following situations, we may disclose your protected health information if you do not object.

Notification.
We may use or disclose information to notify or assist in notifying a family member, or friend of your location and general condition.

Communications.
Staff members may disclose to a family member, other relative, or close personal friend health information relevant to that person's involvement in your care or payment related to your care.
If you are present for, or otherwise available prior to, a notification or communication with family or another caregiver, and you have the capacity to make health care decisions, we may make the disclosure if you agree; or if we provide you with the opportunity to object and you do not object; or we reasonably infer from the circumstances that you do not object. If you are not present for the notification or disclosure, or the opportunity to agree or object cannot be provided because of your incapacity or an emergency circumstance, we may determine whether the disclosure is in your best interest and, if so, we may disclose to the designated person only that information that is directly relevant to the person's involvement with your health care.

VI. Uses and Disclosures Not Requiring Your Authorization.
The federal privacy rules provide that we may use or disclose your protected health information without your authorization in the following circumstances:

Food and Drug Administration (FDA):
We may disclose to the FDA health information relative to adverse events with respect to food, supplements, product and product defects, or post marketing surveillance information to enable product recalls, repairs, or replacement.

Workers Compensation:
We may disclose health information to the extent authorized by and to the extent necessary to comply with laws relating to workers compensation or other similar programs established by law.

Public Health:
As required by law, we may disclose your health information to public health or legal authorities charged with preventing or controlling disease, injury, or disability.

Correctional Institution:
Should you be an inmate of a correctional institution or a resident of another form of court-ordered placement (for example, if you are involuntarily committed to the developmentally disabled system), we may disclose to the institution or agents thereof health information necessary for your health and the health and safety of other individuals.

Law Enforcement:
We may disclose health information for law enforcement purposes as required by law or in response to a valid search warrant or court order.

Criminal Activity:
We may disclose your protected health information if we believe that it constitutes evidence of criminal conduct that occurred on our premises. We may also disclose your protected health information if we are required by applicable state law to report

suspected child abuse or neglect or abuse of incapacitated adults or an injury that we believe may have been the result of an illegal act. We may also disclose protected health information if it is necessary for law enforcement authorities to identify or apprehend an individual.

Legal Proceedings:
We may disclose protected health information in the course of any judicial or administrative proceeding, in response to an order of a court or administrative tribunal (to the extent such disclosure is expressly authorized), and, in certain situations, in response to a subpoena, discovery request or other lawful process.

Relating to Decedents:
We may disclose protected health information regarding an individual's death to coroners, medical examiners or funeral directors consistent with applicable law.

As Required By Law:
We may use or disclose your protected health information to the extent that the use or disclosure is required by state or federal law. The use or disclosure will be made in compliance with the law and will be limited to the relevant requirements of the law. For example, we must make disclosures when required by the Secretary of the Department of Health and Human Services to investigate or determine our compliance with the requirements of the federal Privacy Rules.

VII. Uses and Disclosures of Protected Health Information Based upon Your Written Authorization
Other uses and disclosures of your protected health information will be made only with your written authorization, unless otherwise permitted or required by law as described in this Notice. You may revoke this authorization, at any time, in writing, except to the extent that we have already relied upon your authorization in making a disclosure.

VIII. HIPAA Safeguards and Mitigation of Harm

We use appropriate safeguards to prevent the use or disclosure of PHI. We have implemented administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that we create, receive, maintain, or transmit on behalf of a Covered Entity. Such safeguards include:

- Maintaining appropriate clearance procedures and providing supervision to assure that our workforce follows appropriate security procedures;
- Providing appropriate training for our staff to assure that our staff complies with our security policies;
- Making use of appropriate encryption when transmitting PHI over the Internet;
- Utilizing appropriate storage, backup, disposal and reuse procedures to protect PHI;
- Utilizing appropriate authentication and access controls to safeguard PHI;
- Utilizing appropriate security incident procedures and providing training to our staff sufficient to detect and analyze security incidents; and
- Maintaining a current contingency plan and emergency access plan in case of an emergency to assure that the PHI we hold on behalf of a Covered Entity is available when needed.

In the event of a use or disclosure of PHI that is in violation of the requirements of the HIPAA Compliance, we will mitigate, to the extent practicable, any harmful effect resulting from the violation. Such mitigation will include:

- Reporting any use or disclosure of PHI and any security incident of which we become aware as the Covered Entity; and
- Documenting such disclosures of PHI and information related to such disclosures as would be required for Covered Entity to respond to a request for an accounting of disclosure of PHI in accordance with HIPAA.

IX. Potential Impact of State Law

The HIPAA Privacy Regulations, generally do not "preempt" (or take precedence over) state privacy or other applicable laws that provide individuals greater privacy protections. As a result, to the extent state law applies, the privacy laws of a particular state, or other federal laws, rather than the HIPAA Privacy Regulations, might impose a privacy standard under which we will be required to operate. For example, where such laws have been enacted, we will follow more stringent state privacy laws that relate to uses and disclosures of protected health information concerning HIV, AIDS, mental health, substance abuse/chemical dependency, genetic testing, reproductive rights, etc.

X. For More Information or to Report Complaints

If you wish to exercise any of the rights listed in Section II of this Notice, or if you have questions and would like additional information you may contact our Privacy Officer either in writing or by phone:

Senior Human Resources Director
Gateways Community Services
144 Canal Street Nashua NH 03064
(603) 459-2717

If you believe that your privacy rights have been violated, you may file a complaint with our Privacy Officer or with the Secretary of the United States Department of Health and Human Services. We will not retaliate against you for filing a complaint.

