

222 Salem Ave.
Dayton, Ohio 45406
(937) 223-8246 Fax (937) 222-6307

NOTICE OF PRIVACY PRACTICES

Effective Date: April 14, 2003

SENIOR RESOURCE CONNECTION

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.

If you have any questions about this notice, please contact our HIPAA Privacy Officer at 937-223-8246, ext 215, 222 Salem Avenue, Dayton, Ohio 45406.

WHO WILL FOLLOW THIS NOTICE:

This notice describes our agency's practices and that of:

- Any health care professional authorized to enter information into your patient chart/record
- All programs of this agency
- All employees, staff and other agency personnel
- All these entities, sites and locations follow the terms of this notice. In addition, these entities, sites and locations may share medical information with each other for treatment, payment or agency operation purpose described in this notice.

OUR PLEDGE REGARDING PROTECTED HEALTH INFORMATION:

We understand that all health information about you is personal and confidential. We are committed to protecting all medical information about you. We create a record of care and services you receive, and use this record to provide you with quality care and to comply with certain legal requirements. This notice applies to all of the records of your care generated by this agency.

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 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 and related health care services.

We are required to abide by the terms of this Notice of Privacy Practices. We may change our notice, at any time. The new notice will be effective for all protected health information maintained at that time.

Upon your request, we will provide you with any revised Notice of Privacy by calling the office to request that a revised copy be sent to you in the mail or asking for one at the time of your next visit.

We also describe your rights and certain obligations we have regarding the use and disclosure of protected health information.

We are required by law to:

- Make sure that medical information that identifies you is kept private.
- Give you notice of our legal duties and privacy practices with respect to medical information about you.
- Follow the terms of the notice that is currently in effect.

I. USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION:

Once you have given your consent, the following categories describe different ways that we use and disclose medical information. For each category of uses or disclosures we will explain what we mean and try to give some examples. Not every use or disclosure in a category will be listed. However, all the ways we are permitted to use and disclose information will fall within one of these categories.

1. For Treatment. We may use medical information about you to provide you with medical treatment or services. We may disclose medical information about you to doctors, nurses, health personnel or other agency personnel involved in taking care of you. For example, a doctor treating you for a broken leg may need to know if you have diabetes because diabetes may slow the healing process. . Different areas of this agency also may share medical information about you in order to coordinate the different things you need, such as prescriptions, lab work, x-rays. We also may disclose medical information about you to another provider outside the agency who may be involved in your medical care after you leave the agency, such as family members, or others we use to provide services (i.e., home health aides, physical therapists, specialists, or other community resources) that are part of your care.
2. For Payment. We may use and disclose medical information about you so that the treatment and services you receive at this agency may be billed to and payment may be collected from you, an insurance company or a third party. For example, we may need to give your health plan information about care you received so that your health plan will pay us or reimburse you for said care. We may also tell your health plan about a treatment you are going to receive to obtain prior approval or to determine whether your plan will cover the treatment.
3. For Health Care Operations. We may use and disclose medical information about you for health care operations. These uses and disclosures are necessary to run the agency and make sure that all of our patients receive quality care. For example, we may use medical information to review our treatment and services, for quality assurance activities, and to evaluate the performance of our staff in caring for you. We may also combine medical information about several patients to decide what additional services the agency should offer, what services are not needed, and whether certain new treatments are effective.
4. Treatment Alternatives. We may use and disclose medical information to tell you about or recommend possible treatment options or alternatives that may be of interest to you.
5. Health Related Benefits and Services. We may use and disclose medical information to tell you about health-related benefits or services that may be of interest to you. This may be in the form of newsletters or brochures mailed to your residence.
6. Individuals Involved in Your Care or Payment for Your Care. We may release medical information about you to a family member who is involved in your medical care. We may also give information to someone who helps pay for your care. In addition, we may disclose medical information about you to an entity assisting in a disaster relief effort so that your family can be notified about your condition, status and location.
7. Business Associates. We will share your protected health information with third party “business associates” that facilitate activities (i.e., billing, transcription services, and lab tests) for this agency. Whenever an arrangement between this agency and a business associate involves the use of disclosure of your protected health information, a written contract that contains terms that will protect the privacy of your protected health information will be in place.
8. As Required by Law. We will disclose medical information about you when required to do so by federal, state or local law.
9. To Avert a Serious Threat to Health or Safety. We may use and disclose medical information about you when necessary to prevent a serious threat to your health and safety or health and safety of the public or another person. Any disclosures, however, would only be to someone able to help prevent the threat

II. SPECIAL SITUATIONS:

1. Organ and Tissue Donation. If you are an organ donor, we may release medical information to agencies that handle organ procurement of organ, eye or tissue transplantation or to an organ donation bank, as necessary to facilitate organ or tissue donation and transplantation.
2. Military or Veterans. If you are a member of the armed forces, we may release protected health information about you as required by military command authorities. We may also release medical information about foreign military personnel to the appropriate foreign military authority. We may use and disclose to components of the Department of Veterans Affairs protected health information about you to determine whether you are eligible for certain benefits.
3. Workers’ Compensation. We may release medical information about you for workers’ compensation or similar programs. These programs provide benefits for work-related injuries or illnesses.
4. Public Health Risks. We may disclose medical information about you for public health activities. These activities generally include the following:
 - To prevent or control disease, injury or disability.
 - To report births and deaths.
 - To report child abuse or neglect.
 - To report reactions to medications or problems with products.
 - To notify people of recalls of products they may be using.
 - To notify a person who may have been exposed to a disease or may be at risk for contracting or spreading a disease or condition.

- To notify the appropriate government authority if we believe a patient has been the victim of abuse, neglect, or domestic violence. We will only make this disclosure if you agree or when required or authorized by law.
- 5. Health Oversight Activities. We may disclose medical information to a health oversight agency for activities authorized by law. These oversight activities include, for example, audits, investigations, inspections, and licensure. These activities are necessary for the government to monitor the health care system, government programs, and compliance with civil rights laws.
- 6. Lawsuits and Disputes. If you are involved in a lawsuit or dispute, we may disclose medical information about you in response to a court or administrative order. We may also disclose medical information about you in response to a subpoena, discovery request, or other lawful process by someone else involved in the dispute, but only if efforts have been made to tell you about the request or to obtain an order protecting the information requested.
- 7. Law Enforcement. We may release medical information if asked to do so by a law enforcement official:
 - In response to a court order, subpoena, warrant, summons or similar process.
 - To identify or locate a suspect, fugitive, material witness, or missing person.
 - About the victim of a crime, if, under certain limited circumstances, we are unable to obtain the person's agreement.
 - About a death we believe may be the result of criminal conduct.
 - About criminal conduct at the agency.
 - In emergency circumstances to report a crime, the location of the crime or victims, or the identity, description or location of the person who committed the crime.
- 8. Coroners, Medical Examiners and Funeral Directors. We may release medical information to a coroner or medical examiner. This may be necessary, for example, to identify a deceased person or determine the cause of death. We may also release medical information about patients of the hospital to funeral directors as necessary to carry out their duties.
- 9. National Security and Intelligence Activities. We may release medical information about you to authorized federal officials for intelligence, counterintelligence, and other national security activities authorized by law.
- 10. Protective Services for the President and Others. We may disclose medical information about you to authorized federal officials so they may provide protection to the President, other authorized persons or foreign heads of state or conduct special investigations.
- 11. Inmates. If you are an inmate of a correctional institution or under the custody of a law enforcement official we may release medical information about you to the correctional institution or law enforcement official. This release would be necessary (1) for the institution to provide you with health care, (2) to protect your health and safety or the health and safety of others, or (3) for the safety and security of the correctional institution.

III. Your Rights Regarding Protected Health Information.

The following is a statement of your rights with respect to your protected health information and description of how you may exercise these rights.

- Right to Request Restrictions. You have the right to request a restriction or limitation on the medical information we use or disclose about you for treatment, payment or health care operations. You also have the right to request a limit on the medical information we disclose about you to someone who is involved in your care or the payment for your care, like a family member or friend. For example, you could ask that we not use or disclose information about a surgery that you had.

We are not required to agree to your request. If we do agree, we will comply with your request unless the information is needed to provide you emergency treatment.

To request restriction, you must make your request in writing to **Senior Resource Connection, HIPAA Privacy Officer, 222 Salem Avenue, Dayton, Ohio 45406**. In your request, you must tell us (1) what information you want to limit, (2) whether you want to limit our use, disclosure or both, and (3) to whom you want the limits to apply, for example, disclosure to your spouse.

- Right to Request Confidential Communications. You have the right to request that we communicate with you about medical matters in a certain way or at a certain location. For example, you can ask that we only contact you at work or by mail.

To request confidential communications, you must make your request in writing to the HIPAA Privacy Officer (see business address in the preceding paragraph, in bold type). We will not ask you the reason for your request. We will accommodate all reasonable requests. Your request must specify how or where you wish to be contacted.

- Right to Inspect and Copy. You have the right to inspect and copy information that may be used to make decisions about your care. Usually, this includes medical and billing records, but does not include psychotherapy notes.

To inspect and copy medical information that may be used to make decisions about you, you must submit your request in writing to HIPAA Privacy Officer (see business address above in the bold type). SRC has 30 days to process your request. If you request a copy of the information, we may charge a fee for the costs of copying, mailing or other supplies associated with your request.

- Right to Amend. If you feel that medical information we have about you is incorrect or incomplete, you may ask us to amend the information. You have the right to request an amendment for as long as the information is kept by or for this agency.

To request an amendment, your request must be made in writing and submitted to the HIPAA Privacy Officer. In addition, you must provide a reason that supports your request. SRC has 60 days to act on said request.

We may deny your request for an amendment if it is not in writing or does not include a reason to support the request. In addition, we may deny your request if you ask us to amend information that:

- Was not created by us, unless the person or entity that created the information is no longer available to amendment.
 - Is not part of the medical information kept by our agency.
 - Is not part of the information which you would be permitted to inspect and copy; or
 - Is inaccurate and complete.
 - SRC will provide written notice of denial. You may file a written statement of disagreement to be placed with the denial in your medical record.
- Right to an Accounting of Disclosures. You have the right to request an “accounting disclosures” made of a provider in the six (6) years prior to your request. This is a list of the disclosures we made of health information about you, and not disclosures to carry out TPO (treatment, payment, and health care operations).

To request this list or accounting of disclosures, you must submit your request in writing to the HIPAA Privacy Officer. Your request must state a time period, which may not be longer than six years and may not include dates before April 16, 2003. Your request should indicate in what form you want the list (for example, on paper, electronically). The first list you request within a 12-month period will be free. For additional lists, we may charge you the cost of providing the list. We will notify you of the cost involved and you may choose to withdraw or modify your request at that time before any costs are incurred.

- Right to a Paper Copy of This Notice. You have the right to a paper copy of this notice. A copy of this notice will be provided to you on your next supervisory visit, after April 14, 2003 (effective date of Privacy Standards). Copies will be available at SRC for any individual to request.

IV. CHANGES TO THIS NOTICE.

We reserve the right to change this notice. We reserve the right to make the revised or changed notice effective for health information we already have about you as well as any information we receive in the future. The notice will contain on the first page, in the top right-hand corner, the effective date. Whenever the notice is revised, it will be available upon request on or after the effective date of revision.

V. COMPLAINTS.

If you believe your privacy rights have been violated, you may file a complaint with our HIPAA Privacy Officer. To file complaints, contact the HIPAA Privacy Officer, at 937-223-8246. All complaints must be submitted in writing to Senior Resource Connection, HIPAA Privacy Officer, 222 Salem Avenue, Dayton OH 45406.

You will not be penalized for filing a complaint.

VI. OTHER USES OF MEDICAL INFORMATION.

Other uses and disclosures of medical information not covered by this notice or the laws that apply to us will be made only with your written permission. If you provide us permission to use or disclose medical information about you, you may revoke that permission, in writing, at any time. If you revoke your permission, we will no longer use or disclose medical information about you for the reasons covered by your written authorization. You understand that we are unable to take back any disclosures we have already made with your permission, and that we are required to retain our records of the care that we provided to you.

VII. BREACH OF INFORMATION

1. Discovery of Breach: A breach of PHI will be treated as “discovered” as of the first day on which such breach is known to the agency, or, by exercising reasonable diligence would have been known to the agency (includes breaches by the agency’s business associates).
2. Breach Investigation: The agency will name an individual to act as the investigator of the breach. The investigator will be responsible for the management of the breach investigation, completion of a risk assessment, and coordinating with others in the agency as appropriate. All documentation related to the breach investigation, including the risk assessment, will be retained for a minimum of six years.
3. Risk Assessment: For an acquisition, access, use or disclosure of PHI to constitute a breach, it must constitute a violation of the Privacy Rule. A use or disclosure of PHI that is incident to an otherwise permissible use or disclosure and occurs despite reasonable safeguards and proper minimum necessary procedures would not be a violation of the Privacy Rule and would not qualify as a potential breach. The agency will need to perform a risk assessment to determine if there is significant risk of harm to the individual as a result of the impermissible use or disclosure. Based on the outcome of the risk assessment, the agency will determine the need to move forward with breach notification.
4. Timeliness of Notification: Upon determination that breach notification is required, the notice will be made without unreasonable delay and in no case later than 60 calendar days after the discovery of the breach by the agency involved or the business associate involved. It is the responsibility of the agency to demonstrate that all notifications were made as required, including evidence demonstrating the necessity of delay.
 - a. Exception: delay for law enforcement purposes.
5. Methods of Notification: The method of notification will depend on the individuals/entities to be notified. The following methods will be utilized accordingly:
 - a. Notice to Individuals
 - b. Notice to Media
 - c. Notice to HHS
6. Maintenance of Breach Information/Log: As described above and in addition to the reports created for each incident, the agency will maintain a process to record or log all breaches of unsecured PHI regardless of the number of patients affected.
7. Workforce Training: The agency will train all members of its workforce on the policies and procedures with respect to PHI as necessary and appropriate for the members to carry out their job responsibilities. Workforce members will also be trained as to how to identify and report breaches within the agency.
8. Retaliation/Waiver: The agency may not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for the exercise by the individual of any privacy right. The agency may not require individuals to waive their privacy rights under as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.