

death. PHI may be used and disclosed for cadaver organ, eye or tissue donation purposes.

Research: Under certain circumstances, we may disclose your PHI to researchers when an institutional review board that has reviewed the research proposal and established protocols to ensure the privacy of your PHI has approved their research.

Criminal Activity: Consistent with applicable federal and state laws, we may disclose your PHI, if we believe that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public. We may also disclose PHI if it is necessary for law enforcement authorities to identify or apprehend an individual.

Military Activity and National Security: When the appropriate conditions apply, we may use or disclose PHI of individuals who are Armed Forces personnel (1) for activities deemed necessary by appropriate military command authorities; (2) for the purpose of a determination by the Department of Veterans Affairs of your eligibility for benefits, or (3) to foreign military authority if you are a member of that foreign military service. We may also disclose your PHI to authorized federal officials for conducting national security and intelligence activities, including for the provision of protective services to the President or others legally authorized.

Workers' Compensation: We may disclose your PHI as authorized to comply with workers' compensation laws and other similar legally-established programs that provide benefits for work-related illnesses and injuries.

Inmates: We may use or disclose your PHI if you are an inmate of a correctional facility and your care provider(s) created or received your protected health information in the course of providing care to you.

Required Uses and Disclosures: Under the law, we must make disclosures to you and when required by the Secretary of the Department of Health and Human Services to investigate or determine our compliance with the requirements of the final rule on Standards for Privacy of Individually Identifiable Health Information.

3. Your Rights Regarding Health Information About You

The following is a statement of your rights with respect to your PHI and a brief description of how you may exercise these rights.

You have the right to inspect and copy your PHI. This means you may inspect and obtain a copy of your PHI contained in your medical and billing records and any other records that your care provider(s) uses for making decisions about you, for as long as we maintain the PHI. We will provide you with access to the protected health information in the form and format you request, if it is readily producible in such form and format; or, if not, we will provide the information in a readable electronic form and format as agreed to by you and us.

To inspect and copy your medical information, you must submit a written request to the Privacy Officer listed on the first and last pages of this Notice. If you request a copy of your information, we may charge you a fee for the costs of copying, mailing or other costs incurred by us in complying with your request.

We may deny your request in limited situations specified in the law. For example, you may not inspect or copy psychotherapy notes; or information compiled in reasonable anticipation of, or use in, a civil, criminal, or administrative action or proceeding, and certain other specified PHI defined by law. In some circumstances, you may have a right to have this decision reviewed. The person conducting the review will not be the person who initially denied your request. We will comply with the decision in any review. Please contact our Privacy Officer if you have questions about access to your medical record.

You have the right to request a restriction of your PHI. This means you may ask us not to use or disclose any part of your PHI for the purposes of treatment, payment or healthcare operations. You may also request that any part of your PHI not be disclosed to family members or friends who may be involved in your care or for notification purposes as described in this Notice of Privacy Practices. Your request must state the specific restriction requested and to whom you want the restriction to apply.

Your care provider(s) is not usually required to agree to a restriction that you may request. If the law allows and the care provider(s) believes it is in your best interest to permit use and disclosure of your PHI, your PHI will not be restricted. If your care provider(s) does agree to the requested restriction, we may not use or disclose your PHI in violation of that restriction unless it is needed to provide emergency treatment. With this in mind, please discuss any restriction you wish to request with your care provider(s). You may request a restriction by our Privacy Officer in writing. In a case where you pay for your services "out of pocket" and there is no submission to a health plan, you can request that we not disclose information to a health plan in this situation and we are required to comply.

You have the right to request to receive confidential communications from us by alternative means or at an alternate location. We will accommodate reasonable requests.

We may also condition this accommodation by asking you for information as to how payment will be handled or specification of an alternative address or other method of contact. We will not request an explanation from you as to the basis for the request. Please make this request in writing to Dianne Kiernan at Sampson's Prosthetic & Orthotic Laboratory, 1737 State Street, Schenectady, New York 12304-1832.

You may have the right to have your care provider(s) amend your protected health information. This means you may request an amendment of your protected health information contained in your medical and billing records and any other records that your care provider(s) uses for making decisions about you, for as long as we maintain the PHI. You must make your request for amendment in writing to Dianne Kiernan and provide the reason or reasons that support your request. We may deny your request that is not in writing or does not state a reason supporting the request. We may deny your request for an amendment of any information that:

1. Was not created by us, unless the person that created the information is no longer available to amend the information;
2. Is not part of the PHI kept by or for us;
3. Is not part of the information you would be permitted to inspect or copy; or
4. Is accurate and complete.

If we deny your request for amendment, we will do so in writing and explain the basis for the denial. You have the right to file a written statement of disagreement with us. We may prepare a rebuttal to your statement and will provide you with a copy of any such rebuttal. Please contact Dianne Kiernan if you have questions about amending your medical record.

You have the right to receive an accounting of certain disclosures we have made, if any, of your PHI. This right only applies to disclosures for purposes other than treatment, payment or healthcare operations as described in this Notice of Privacy Practices. It also excludes disclosures we may have made to you, to family members or friends involved in your care, or for notification purposes. You have the right to receive specific information regarding these disclosures that occurred after **9/1/2013**. The right to receive this information is subject to certain exceptions, restrictions and limitations. You must submit a written request for disclosures in writing to the Privacy Officer. You must specify a time period, which may not be longer than six years and cannot include any date before **9/1/2013**. You may request a shorter timeframe. Your request should

indicate the form in which you want the list (i.e., on paper, etc). You have the right to one free request within any 12-month period, but we may charge you for any additional requests in the same 12-month period. We will notify you about the charges you will be required to pay, and you are free to withdraw or modify your request in writing before any charges are incurred.

You have the right to obtain a paper copy of this notice from us, upon request to our Privacy Officer, or in person at our office, at any time, even if you have agreed to accept this notice electronically.

4. Complaints

The patient has the right to freely voice grievances and recommend changes in care or services without fear of reprisal or unreasonable interruption of services. You may complain to us or to the Secretary of the Office of Civil Rights of Health and Human Services if you believe your privacy rights have been violated by us. You may file a complaint with us by notifying our Privacy Officer of your complaint. We will not retaliate against you in any way for filing a complaint, either with us or with the Secretary.

You may contact our patient advocate, Dianne Kiernan, in writing at 1737 State Street, Schenectady, New York 12304-1832 for further information about the complaint process.

5. Data Breach

In the event we become aware of a breach of data, we will notify the affected parties in accordance with our HITECH Breach Notification Policy.

6. Notification in the Case of a Breach

(a) **In General.**—Upon discovery of a Breach of Protected Health Information for which we are responsible, we will notify each individual whose unsecured protected health information has been, or we reasonably believe has been, accessed, acquired, or disclosed as a result of such breach.

(b) **Notification by Business Associate.**—A business associate that accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses unsecured protected health information shall, following the discovery of a breach of such information, notify us of such breach. Such notice shall include the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the business associate to have been, accessed, acquired, or disclosed during such breach.

(c) **Breaches Treated as Discovered.**—For purposes of this section, a breach shall be treated as discovered by us or by our business associate as of the first day on which such breach is known to us or our associate, respectively, (including any person, other than the individual committing the breach, that is an employee, officer, or other agent of such entity or associate, respectively) or should reasonably have been known to such entity or associate (or person) to have occurred.

(d) **Timeliness of Notification.**—

(1) **In General.**—Subject to subsection (g), all notifications required under this section shall be made without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach by us (or business associate involved in the case of a notification required under subsection (b)).

(2) **Burden of Proof.**—We will document that all notifications were made as required under this part, including evidence demonstrating the necessity of any delay.

(e) **Methods of Notice.**—

(1) **Individual Notice.**—Notice required under this section to be provided to an individual, with respect to a breach, shall be provided promptly and in the following form:

(A) Written notification by first-class mail to the individual (or the next of kin of the individual if the individual is deceased) at the last known address of the individual or the next of kin, respectively, or, if specified as a preference by the individual, by electronic mail. The notification may be provided in one or more mailings as information is available.

(B) In the case in which there is insufficient, or out-of- date contact information

(including a phone number, email address, or any other form of appropriate communication) that precludes direct written (or, if specified by the individual under subparagraph (A), electronic) notification to the individual, a substitute form of notice shall be provided, including, in the case that there are 10 or more individuals for which there is insufficient or out-of-date contact information, a conspicuous posting for a period determined by the Secretary on our website home page or notice in major print or broadcast media, including major media in geographic areas where the individuals affected by the breach likely reside. Such a notice in media or web posting will include a toll-free phone number where an individual can learn whether or not the individual's unsecured protected health information is possibly included in the breach.

(C) In any case where we determine that possible imminent misuse of unsecured protected health information requires urgency, we in addition to notice provided under subparagraph (A), may provide information to individuals by telephone or other means, as appropriate.

(2) **Media Notice.**—Notice shall be provided to prominent media outlets serving a State or jurisdiction, following the discovery of a breach described in subsection (a), if the unsecured protected health information of more than 500 residents of such State or jurisdiction is, or is reasonably believed to have been, accessed, acquired, or disclosed during such breach.

(3) **Notice to Secretary.**—We will provide notice to the Secretary if we experience a breach. If the breach was with respect to 500 or more individuals then such notice shall be provided immediately. If the breach was with respect to less than 500 individuals, we will maintain a log of any such breach occurring and annually submit such a log to the Secretary documenting such breaches occurring during the year involved.

(f) **Content of Notification.**—Regardless of the method by which notice is provided to individuals under this section, notice of a breach shall include, to the extent possible, the following:

(1) A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.

(2) A description of the types of unsecured protected health information that were involved in the breach (such as full name, Social Security number, date of birth, home address, account number, or disability code).

(3) The steps individuals should take to protect themselves from potential harm resulting from the breach.

(4) A brief description of what we are doing to investigate the breach, to mitigate losses, and to protect against any further breaches.

(5) Contact procedures for individuals to ask questions or learn additional information, which shall include a toll free telephone number, an e-mail address, web site, or postal address.

(g) **Delay of Notification Authorized for Law Enforcement Purposes.**—If a law enforcement official determines that a notification, notice, or posting required under this section would impede a criminal investigation or cause damage to national security, such notification, notice, or posting shall be delayed in the same manner as provided under section 164.528(a)(2) of title 45, Code of Federal Regulations, in the case of a disclosure covered under such section.

(h) **Unsecured Protected Health Information.**—

(1) **Definition.**—The term "unsecured protected health information" shall mean protected health information that is not secured by a technology standard that renders protected health information unusable, unreadable, or indecipherable to unauthorized individuals and is developed or endorsed by a standards developing organization that is accredited by the American National Standards Institute.

7. Changes to This Notice

We reserve the right to change the privacy practices that are described in this Notice of Privacy Practices. We also reserve the right to apply these changes retroactively to PHI received before the change in privacy practices. You may obtain a revised Notice of Privacy Practices by calling the office and requesting a revised copy be sent in the mail, asking for one at the time of your next appointment, or accessing our website.

This notice was published and becomes effective on November 14, 2014.

Our Commitment to Protecting Your Health Information

This Notice of Privacy Practices describes how we may use and disclose your Protected Health Information (“PHI”) 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 PHI. Your “protected health information” means any of your written or oral health information, including demographic data that can be used to identify you. This is health information that is created or received by your health care provider that relates to your past, present or future physical or mental health or condition. We are strongly committed to protecting your PHI. We create a medical record about your care because we need the record to provide you with appropriate treatment and to comply with various legal requirements. We transmit some medical information about your care in order to obtain payment for the services you receive and we use certain information in our day-to-day operations. This Notice will let you know about the various ways we use and disclose your medical information and describe your rights and our obligations with respect to the use or disclosure of your medical information. We will also ask that you acknowledge receipt of this Notice the first time you come to or use any of our facilities, or submit a new prescription because the law requires us to make a good faith effort to obtain your acknowledgment.

We are required by law to:

Make sure that any medical or health information that we have that identifies you is kept private, and will be used or disclosed only in accordance with this Notice of Privacy Practices and applicable law;

Notify you in the event of a breach of any unsecured protected health information if your information has been compromised;

Give you this Notice of our legal duties and our privacy practices with respect to the protected health information; and
Abide by the terms of the Notice of Privacy Practices that is in effect from time to time.

2. Uses and Disclosures of Protected Health Information

A. Uses and Disclosures of Protected Health Information for Treatment, Payment and Healthcare Operations

Your PHI may be used and disclosed by your care provider(s), our office staff and others outside of our office that are involved in your care and treatment for the purpose of providing health care services to you. Your PHI may also be used and disclosed to secure payment for your health care bills.

The following are examples of the types of uses and disclosures of your protected health information that this facility is permitted to make. We have provided some examples of the types of each use or disclosure we may make, but not every use or disclosure in any of the following categories will be listed.

For Treatment: We will use and disclose your PHI to provide, coordinate, or manage your health care and any related treatment. 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 PHI. For example, we would disclose your PHI, as necessary, to the physician that referred you to us. We will also disclose PHI to other health care providers who may be treating you when we have the necessary permission from you to disclose your PHI.

For Payment: Your PHI will be used, as needed, to obtain payment for your health care services. This may include certain activities that your health insurance plan may undertake before it approves or pays for the health care services we recommend for you such as; making a determination of eligibility or

coverage for insurance benefits, reviewing services provided to you for medical necessity, and undertaking utilization review activities. We may also tell your health plan about a health care item or service you are going to receive in order to obtain prior approval or to determine whether your plan will cover the device. However, we will not provide protected health information pertaining solely to a health care item or service for which you, or a person other than the health plan, on your behalf, have paid us in full.

For Healthcare Operations: We may use or disclose, as needed, your PHI in order to support the business activities of this facility. These activities include, but are not limited to, quality assessment activities, employee review activities, legal services, licensing, and conducting or arranging for other business activities. We may share your PHI with third party “business associates” that perform various activities (e.g., satisfaction surveys, healthcare outcomes surveys, billing, transcription, accreditation services, and/or performance tracking surveys) for this facility. Whenever an arrangement between our facility and our business associate involves the use or disclosure of your PHI, we will have a written contract that contains terms that will protect the privacy of your PHI.

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

Appointment Reminders: We may use or disclose your PHI, as necessary, to contact you to remind you of your appointment.

Sign-In Sheets: We may use a sign-in sheet at the registration desk where you will be asked to sign your name. We may also call you by name in the waiting room when your care provider(s) is ready to see you.

Sale of the Practice: If we decide to sell this practice or merge or combine with another practice, we may share your PHI with the new owners.

B. Uses and Disclosures of Protected Health Information based upon your written authorization

Other uses and disclosures of your PHI will be made only with your written authorization, unless otherwise permitted or required by law as described below. You may revoke your authorization, at any time, in writing. You understand that we cannot take back any use or disclosure we may have made under the authorization before we received your written revocation, and that we are required to maintain a record of the medical care that has been provided to you. The authorization is a separate document, and you will have the opportunity to review any authorization before you sign it. We will not condition your treatment in any way on whether or not you sign any authorization.

C. Other Permitted and Required Uses and Disclosures that may be made either with your agreement or your opportunity to object

We may use and disclose your PHI in instances where you have the opportunity to agree or object to the use or disclosure of all or part of your PHI. If you are not present or able to agree or object to the use or disclosure of the PHI, then your care provider(s) may, using their professional judgment, determine whether the disclosure is in your best interest. In this case, only the PHI that is relevant to your health care will be disclosed.

Others Involved in Your Healthcare: Unless you object, we may disclose to a member of your family, a relative, a close friend or any other person you identify, orally or in writing, your PHI that directly relates to that person's involvement in your health care. If you are unable to agree or object to such a disclosure, we may disclose such information as necessary if we determine that it is in your best interest based on our professional judgment. We may use or disclose your PHI to notify or assist in notifying a family member, personal representative or any other person that is responsible for your care of your location or general condition.

D. Other Permitted and Required Uses and Disclosures that may be made without your authorization or opportunity to object

We may use or disclose your PHI in the following situations without your authorization or providing you the opportunity to object:

Required By Law: We may use or disclose your PHI to the extent that federal, state or local law requires the use or disclosure. The use or disclosure will be made in compliance with the law and will be limited to the relevant requirements of the law. You will be notified, if required by law, of any such uses or disclosures.

Public Health: We may disclose your PHI for public health activities and purposes to a public health authority that is permitted by law to collect or receive the information. The disclosure will be made for the purpose of controlling disease, injury or disability. A disclosure under this exception would only be made to somebody in a position to help prevent the threat to public health.

Communicable Diseases: We may disclose your PHI, if authorized by law, to a person who may have been exposed to a communicable disease or may otherwise be at risk of contracting or spreading the disease or condition.

Health Oversight: We may disclose PHI to a health oversight agency for activities authorized by law, such as audits, investigations, and inspections. Oversight agencies seeking this information include government agencies that oversee the health care system, government benefit programs, other government regulatory programs and civil rights laws.

Abuse or Neglect: We may disclose your PHI to a public health authority that is authorized by law to receive reports of child abuse or neglect. In addition, we may disclose your PHI if we believe that you have been a victim of abuse, neglect or domestic violence to the governmental entity or agency authorized to receive such information. We will only make this disclosure if you agree or when required or authorized by law. In this case, the disclosure will be made consistent with the requirements of applicable federal and state laws.

Military and Veterans: If you are a member of the military, we may release protected health information about you as required by military command authorities.

Food and Drug Administration: We may disclose your PHI to a person or company required by the Food and Drug Administration to report adverse events, product defects or problems, biologic product deviations, track products; to enable product recalls; to make repairs or replacements, or to conduct post marketing surveillance, as required.

Legal Proceedings: We may disclose your PHI 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), in certain conditions in response to a subpoena, discovery request or other lawful process.

Law Enforcement: We may also disclose your PHI, so long as applicable legal requirements are met, for law enforcement purposes. These law enforcement purposes might include (1) legal processes and otherwise required by law, (2) limited information requests for identification and location purposes, (3) pertaining to victims of a crime, (4) suspicion that death has occurred as a result of criminal conduct, (5) in the event that a crime occurs on the premises of the practice, and (6) medical emergency (not on the facility's premises) and it is likely that a crime has occurred.

Coroners, Funeral Directors, and Organ Donation: We may disclose your protected health information to a coroner or medical examiner for identification purposes, determining cause of death or for the coroner or medical examiner to perform other duties authorized by law. We may also disclose PHI to a funeral director, as authorized by law, in order to permit the funeral director to carry out their duties. We may disclose such information in reasonable anticipation of

NOTICE OF PRIVACY PRACTICES

For Sampson's Prosthetic & Orthotic Laboratory

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:
Dianne Kiernan our Privacy Officer at (518) 374-6011.