

NOTICE OF PRIVACY PRACTICES – STRATUS

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 Privacy Officer at the number listed at the end of this Notice.

Each time you visit a healthcare provider, a record of your care is created. Typically, this record contains medical information such as your symptoms, examination, test results, diagnoses, treatment and/or treatment plan and billing-related information. This information is considered protected health information (PHI).

This Notice is intended to advise you about the ways we may use and disclose medical information about you and comply with the Health Insurance Portability and Accountability Act (HIPAA) and the General Data Protection Regulation (GDPR). It also describes your rights and certain obligations with regard to your medical information and applies to all of the records of your care generated by your healthcare provider(s) for our organization.

Our Responsibilities

Stratus and/or its subsidiaries and/or affiliates ("Company") is required to maintain the privacy of your health information and to provide you with a description of our legal duties and privacy practices regarding your health information that we collect and maintain.

We are required by law to abide by the terms of this Notice and notify you if changes are made. We reserve the right to make changes to the Notice and make the new provisions effective for all protected health information we maintain. Copies of our Notice are available in our patient packets, our facilities and on our website.

To comply with the GDPR, Stratus applies data protection principles designed to ensure that personal data is:

- processed lawfully, fairly and transparently;
- collected for specified, explicit and legitimate purposes;
- adequate, relevant and limited to what is necessary;
- accurate and, where necessary, kept up to date;
- kept only for as long as necessary for the relevant purposes and legal requirements; and
- protected using appropriate technical and organizational safeguards.

We support these principles through governance activities such as data mapping, lawful-basis review, internal policies and procedures, privacy and security policy maintenance and incident response processes.

Personal data we collect

We may collect the following categories of personal data, depending on your relationship with us and the services provided:

- Identity and contact data: name, date of birth, gender, address, telephone number, email address, patient or account identifiers, government or insurance identifiers where relevant.
- Health and clinical data: symptoms, diagnoses, medical history, examination notes, test results, monitoring data, treatment plans, prescriptions, referrals, clinician notes and other information needed to provide or support healthcare services.
- Special category data: health data and, where relevant to care or legal requirements, information revealing racial or ethnic origin, sex life or sexual orientation, genetic data, biometric data or disability-related information.
- Payment and insurance data: billing details, payment history, insurer or third-party payer details, eligibility, referrals, pre-authorizations and claims information.
- Communications data: calls, emails, text messages, portal messages, appointment reminders, preferences, complaints and correspondence with you or your authorized representatives.
- Technical and usage data: device information, IP address, browser type, access logs, cookie identifiers, website or portal usage data and security logs.
- Emergency, carer and representative data: details of family members, carers, guardians, attorneys, emergency contacts or other persons authorized to act for or support you.
- Legal and compliance data: consent records, authorizations, identity checks, records of rights requests, incident records, audit logs, regulatory correspondence and litigation or claims information.

How we collect personal data

- Directly from you, including when you register, attend an appointment, complete forms, use a portal or website, call us, email us, text us or otherwise communicate with us.
- From healthcare professionals, hospitals, laboratories, imaging centers, pharmacies, referral sources, care coordinators and other organizations involved in your care.
- From insurers, employers, third-party payers, government programmes, payment processors and billing or collections partners.
- From family members, carers, legal representatives, guardians or other persons you authorize, or where disclosure is permitted by law.

- Automatically through our systems, websites, portals, security tools, access logs and cookies or similar technologies.
- From public authorities, regulators, courts, law enforcement or other third parties where permitted or required by law.

How We May Use and Disclose Medical Information about You

The following describes examples of the way we may use and disclose medical information:

For Treatment: We may use medical information about you to provide, coordinate and manage your treatment or services. We may disclose medical information about you to other healthcare professionals such as physicians, nurses, technicians, clinical laboratories, imaging centers, medical students, or other personnel who are involved in your care.

We may communicate your information using various methods, orally, written, facsimile and electronic communications.

We may also provide other healthcare professionals who contribute to your care with copies of various reports and information to assist him/her and ensure that they have appropriate information regarding your condition/treatment plan and diagnosis.

For Payment: We may use and disclose medical information about your treatment and services to bill and collect payment from you, your insurance company or a third party payer. Examples may include contacting your insurance company for referrals, verification or pre-approval of covered services.

For Health Care Operations: We may use or disclose, as needed, your health information in order to support our business activities. These activities may include, but are not limited to quality assessments, employee review activities, licensing, legal advice, accounting support, information systems support and conducting or arranging for other business activities. We may contact you to remind you of your appointment via personal e-mail, and/ or phone calls, and/or text messaging unless requested to opt out.

Business Associates, BA: Provide services for our organization through written contracts and/or service agreements. Examples of these services include billing and collection and software support. We may disclose your health information to a BA so they can perform the services we have asked them to do such as billing your third-party payer for services rendered. The BA is also required by law to protect and safeguard your health information which is clearly defined through our Business Associate Agreement and written contracts/service agreements.

Breach Notification: In the event that there has been a breach of unsecured protected health information (PHI) identified on behalf of our organization or a BA you will be notified within 60 days of the breach. In addition to your individual notification we may be required to meet further reporting requirements set forth by state and federal agencies. For EU and EEA, a personal data breach is dealt with in accordance with GDPR Articles 33 and 34, where controllers must notify the relevant supervisory authority without undue delay or at least within 72 hours, unless the breach is unlikely to pose a risk to individuals.

Uses and Disclosures That May Be Made *With Your Consent, Authorization or Opportunity to Object*

We will not use and disclose information without your written authorization, except as described in this Notice or as required by applicable laws. Written authorization is required for, most uses and disclosures of psychotherapy notes; PHI for marketing purposes unless we speak with you and disclosures that may constitute a sale of PHI. If you provide an authorization to use or disclose medical information about you, you may revoke that authorization, in writing, at any time. If you revoke your authorization, we will no longer use or disclose medical information about you for the reasons covered by your written authorization. However, we are unable to take back any disclosures we have already made with your authorization.

Individuals Involved in Your Care or Payment for Your Care: Unless you object, we may release medical information about you to a friend or family member who is involved in your medical care or who helps to 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.

Future Communications: We may communicate with you via newsletters, mailings or other means regarding treatment options and information on health-related benefits or services; to remind you that you have an appointment; or other community based initiatives or activities to include limited marketing or fundraising initiatives in which our facility is participating. You have the right to opt out at any time if you are not interested in receiving these communications, please contact our Privacy Officer.

Marketing and Fundraising initiatives, if applicable are limited and may require a separate authorization.

Uses and Disclosures That May Be Made *Without Your Authorization or Opportunity to Object*

We may use or disclose your health information in the following situations without your authorization or without providing you with an opportunity to object. These situations include:

As required by law: We may use and disclose health information to the following types of entities, including but not limited to:

- Food and Drug Administration
- Public Health or Legal Authorities charged with preventing or controlling disease, injury or disability
- Correctional Institutions
- Workers Compensation Agents

- Organ and Tissue Donation Organizations
- Military Command Authorities
- Health Oversight Agencies
- Funeral Directors, Coroners and Medical Directors
- National Security and Intelligence Agencies
- Protective Services for the President and Others
- Authority that receives reports on abuse and neglect

If you are not present, able to agree or object to the use or disclosure (such as in an emergency situation), then your healthcare provider may, using professional judgment, determine whether the disclosure is in your best interest. In this case, only the information that is relevant to your health care will be disclosed.

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

State-Specific Requirements: Many states have reporting requirements which may include population-based activities relating to improving health or reducing health care costs, cancer registries, birth defect registries and others.

International transfers

Stratus is based in the United States and may process or receive personal data in the United States, the United Kingdom, the European Economic Area (EEA), Switzerland, Australia, the Middle East or other countries where Stratus, its affiliates or service providers operate. Where personal data is transferred from the EEA, UK or Switzerland to a country that has not been recognized as providing an adequate level of protection, we will use appropriate transfer safeguards where required, such as the European Commission Standard Contractual Clauses (SCC's), the UK International Data Transfer Agreement or Addendum, adequacy regulations, supplementary measures or another lawful transfer mechanism.

Security

We use appropriate technical and organizational measures designed to protect personal data against unauthorized or unlawful processing and against accidental loss, destruction or damage. Measures may include access controls, authentication, role-based permissions, encryption where appropriate, logging and monitoring, staff training, confidentiality obligations, vendor due diligence, incident response procedures, backups and business continuity arrangements. No system is completely secure, but we work to protect personal data in a way that is appropriate to the risk.

Our data protection compliance program may include data mapping reviews, internal privacy and security policies, workforce procedures, incident response processes, periodic lawful-basis reviews and vendor or processor oversight designed to maintain a consistent approach to data protection across relevant regions.

Automated decision-making and profiling

We do not use personal data to make decisions based solely on automated processing, including profiling, that produce legal effects concerning you or similarly significantly affect you, unless we tell you separately and the processing is permitted by law. [If Stratus uses such systems, insert meaningful information about the logic involved, significance and envisaged consequences, and describe available human review rights.]

Websites, portals and cookies

Our websites and portals, including <https://stratusneuro.com>, may use cookies, pixels, analytics tools and similar technologies. Essential technologies are used to provide and secure the service. Non-essential cookies or analytics will be used only where permitted by applicable law and, where required, with consent. More information should be provided in Stratus's Cookies Policy, including how users can manage their choices.

Your Health Information Rights

Although your health record is the physical property of the organization that compiled it, you have the right to:

Inspect and Copy: You and/or your personal representative have the right to inspect, review and receive a copy of your medical information. Electronic copies are available and may include various electronic means such as a patient portal or other reasonable accommodations requested. We may deny your request to inspect and copy in limited circumstances to include release of psychotherapy notes or information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding. If you are denied access to medical information, you may request that the denial be reviewed.

Requests to copy and/or a review must be submitted in writing to Stratus. There will be a fee charged for all applicable copying and producing copy of portable media (CD, DVD, USB) up to the maximum amount as prescribed by governing law.

Amend: If you feel that the medical information we have is incomplete or incorrect, you may ask us to amend the information by submitting a request in writing providing a reason to support the amendment request. You will be notified of the decision of your request in writing within 60 days.

An Accounting of Disclosures: You have the right to request an accounting of our disclosures of your medical information; the list will not include disclosures to carry out treatment, payment and health care operations. Company will provide the first accounting to you in any 12-month period without charge, upon receipt of your written request. The cost for subsequent requests for an accounting within the 12-month period will be up to the maximum amount prescribed by governing law.

Request Restrictions: You have the right to request a restriction or limitation of your medical information we use or disclose about you for treatment, payment or health care operations. **Restrictions from your health plan (insurance company):** You have the right to request that we restrict disclosure of your medical information to your health plan for covered services; provided the disclosure is not required by other laws and services must be paid in full by you. **Other Restrictions. Limiting Information:** You also have the right to request and limit any medical information we disclose about you to someone who may be involved in your care or the payment of your care, such as a family member or friend. We ask that you submit these requests in writing.

We may not agree or be required to agree to your request(s) for specific reasons, if this occurs, you will be informed of the reason(s) for the denial.

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. We will agree to the request to the extent that it is reasonable for us to do so. For example, you may request that we use an alternate phone number or mailing address. We ask that you submit these requests in writing.

E-mail communication requests if applicable may require a separate authorization.

For EU and EEA:

Individuals within EU and EEA have more rights according to Art.15 – 21 of the GDPR.

Subject to legal limits and verification of your identity, you may have the following rights:

- Right of access: to ask for confirmation that we process your personal data and receive a copy of it.
- Right to rectification: to ask us to correct inaccurate or incomplete personal data.
- Right to erasure: to ask us to delete personal data in certain circumstances.
- Right to restriction: to ask us to limit processing in certain circumstances.
- Right to data portability: to receive certain personal data in a structured, commonly used, machine-readable format and ask us to transmit it to another controller where technically feasible.
- Right to object: to object to processing based on legitimate interests, public task or direct marketing. If you object to direct marketing, we will stop using your data for that purpose.
- Right to withdraw consent: to withdraw consent at any time where we rely on consent.
- Rights relating to automated decision-making: to request human intervention, express your point of view and contest a solely automated decision where these rights apply.
- Right to complain: to lodge a complaint with a data protection supervisory authority.

When you want to exercise any of these rights we may ask for information to verify your identity and clarify your request. We will respond within one month unless the GDPR allows an extension because the request is complex or numerous. We will not discriminate or retaliate against you for exercising your rights. Some rights are not absolute. For example, we may need to retain health records to comply with legal obligations, establish or defend legal claims, support patient safety, maintain accurate clinical records or comply with public health and regulatory duties. We will explain the reason if we cannot fully comply with a request.

To exercise any of your rights, please submit your request in writing to the organization's privacy officer indicated below.

For More Information or to Report a Problem

If you have questions and would like additional information, please contact the Privacy Officer. If you believe that your (or someone else's) privacy rights may have been violated, you may file a complaint with the Privacy Officer at the contact number below or with the Secretary of Health and Human Services at 800-368-1019. Further instructions for filing a complaint can also be found at www.hhs.gov/ocr or with your local EU or EEA Data Protection Authority. All complaints must be submitted in writing within 180 days, or 30 days for EU and EEA members, of when you knew that the act or omission occurred and there will be no retaliation for filing a complaint.

Changes to this notice

We may update this notice from time to time. If we make material changes, we will take appropriate steps to bring the changes to your attention, such as posting the updated notice on our website, making it available at our facilities or contacting you where required by law. The effective date at the end of this notice shows when it was last updated.

Privacy Officer: Compliance Officer

Telephone Number: 469-995-8416

contact@stratusneuro.com

Corporate Office: Stratus

600 Las Colinas Blvd E, Suite 2000

Irving, Texas 75039

Effective Date: July 17, 2026