SMART MEDICAL

NOTICE OF PRIVACY PRACTICES & HIPAA COMPLIANCE POLICY STATEMENT

Effective Date: March 16, 2026 | Last Revised: March 2026

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.

1. INTRODUCTION

Smart Medical is committed to protecting the privacy and security of your Protected Health Information (PHI). As a provider of Durable Medical Equipment (DME) and medical supplies, we are a covered entity under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), as amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, and all applicable regulations promulgated thereunder.

This policy applies to all employees, contractors, vendors, business associates, and any other individuals or entities that access, use, or disclose PHI on behalf of Smart Medical. Compliance with this policy is mandatory and non-negotiable.

2. KEY DEFINITIONS

For purposes of this Policy, the following definitions apply:

Term	Definition
Protected Health Information (PHI)	Any individually identifiable health information that is created, received, maintained, or transmitted by Smart Medical, including demographic information, that relates to a patient's past, present, or future physical or mental health condition, the provision of health care, or payment for health care.
Electronic PHI (ePHI)	PHI that is created, stored, transmitted, or received in electronic form, including records in computer systems, emails, and digital storage devices.
Covered Entity	A health care provider (such as Smart Medical) that transmits health information in electronic form in connection with transactions for which HHS has adopted standards.
Business Associate (BA)	A person or entity that performs certain functions or activities involving the use or disclosure of PHI on behalf of, or in providing services to, Smart Medical.
Minimum Necessary Standard	The principle requiring that uses and disclosures of PHI be limited to the minimum amount necessary to accomplish the intended purpose.

Authorization	A signed, written permission from a patient allowing Smart Medical to use or disclose PHI for purposes beyond treatment, payment, and health care operations.

3. PROTECTED HEALTH INFORMATION WE COLLECT

In the course of providing DME products and services, Smart Medical collects and maintains the following categories of PHI:

3.1 Patient Identification Information

- Full legal name, date of birth, Social Security Number (SSN) or Tax ID
- Home address, telephone numbers, and email addresses
- Insurance member ID, group number, and payer information
- Referring physician and treating provider information

3.2 Clinical & Medical Information

- Diagnoses, ICD-10 codes, and medical conditions necessitating DME
- Physician orders, prescriptions, and certificates of medical necessity (CMN)
- Prior authorization approvals and utilization review documentation
- Functional assessments, home assessments, and clinical notes
- Medication lists when relevant to DME selection or usage

3.3 Financial & Billing Information

- Medicare, Medicaid, and commercial insurance details
- Explanation of benefits (EOB) and claims information
- Payment records, co-pay and deductible information
- Credit card and bank account information (processed via secure PCI-compliant channels)

3.4 Delivery & Equipment Records

- Delivery addresses, delivery confirmations, and proof of delivery (POD)
- Equipment serial numbers, model numbers, and service records
- Repair, maintenance, and compliance monitoring records
- Returns, recalls, and safety-related communications

4. PERMISSIBLE USES AND DISCLOSURES OF YOUR PHI

Smart Medical may use and disclose your PHI for the following purposes without your written authorization, as permitted by HIPAA:

4.1 Treatment

We use and share your PHI with physicians, therapists, home health agencies, hospitals, and other health care providers involved in your care to provide, coordinate, or manage your health care and related services. For example, we share your diagnosis and prescription with our clinical staff to fit and deliver the appropriate DME device.

4.2 Payment

We use and disclose your PHI to obtain payment for the DME products and services we provide. This includes submitting claims to Medicare, Medicaid, and private insurance carriers; verifying insurance eligibility; obtaining prior authorizations; and pursuing collections when necessary.

4.3 Health Care Operations

We use and disclose PHI as necessary for our internal business operations, including but not limited to:

- Quality assessment and improvement activities
- Staff training, competency assessments, and credentialing
- Compliance audits, legal reviews, and risk management
- Business planning, management, and administration
- Accreditation, certification, and licensing activities

4.4 Required by Law

We will disclose your PHI when required to do so by federal, state, or local law, including disclosures to the U.S. Department of Health and Human Services (HHS) for compliance investigations.

4.5 Public Health Activities

We may disclose your PHI to public health authorities for activities such as reporting communicable diseases, reporting adverse events related to medical devices, and notifying manufacturers of FDA-regulated products.

4.6 Abuse, Neglect, and Domestic Violence

We may disclose your PHI to government authorities authorized to receive reports of abuse, neglect, or domestic violence as required or permitted by law.

4.7 Health Oversight Activities

We may disclose your PHI to health oversight agencies such as the Centers for Medicare & Medicaid Services (CMS), the Office of Inspector General (OIG), and state licensing boards for audits, investigations, inspections, and civil, administrative, or criminal proceedings.

4.8 Judicial and Administrative Proceedings

We may disclose your PHI in response to a court order, subpoena, or other lawful process in judicial or administrative proceedings.

4.9 Law Enforcement

We may disclose your PHI to law enforcement officials under certain limited circumstances as required or permitted by applicable law.

4.10 Serious Threats to Health or Safety

We may use or disclose your PHI when necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public.

5. USES AND DISCLOSURES REQUIRING YOUR WRITTEN AUTHORIZATION

The following uses and disclosures require your prior written authorization:

- Most uses and disclosures of psychotherapy notes
- Uses and disclosures of PHI for marketing purposes

- Sale of your PHI to any third party
- Most uses and disclosures not described in this policy

You may revoke any authorization in writing at any time. Your revocation will be effective for future uses and disclosures but will not affect actions taken in reliance on your authorization before it was revoked. Revocation requests should be submitted in writing to our Privacy Officer.

6. YOUR RIGHTS REGARDING YOUR PROTECTED HEALTH INFORMATION

As a patient and customer of Smart Medical, you have the following rights under HIPAA. To exercise any of these rights, please contact our Privacy Officer at the information listed in Section 11.

6.1 Right to Access and Copy Your PHI

You have the right to inspect and receive a copy of your PHI that we maintain in a designated record set. We will respond to your request within 30 days. We may charge a reasonable, cost-based fee for copies. We may deny access in limited circumstances, and you have the right to have any denial reviewed.

6.2 Right to Request Amendment

If you believe that PHI we maintain about you is incorrect or incomplete, you may request that we amend the information. We will respond within 60 days. We may deny the request if the PHI was not created by us, is not part of the designated record set, or is accurate and complete. If we deny your request, you have the right to submit a statement of disagreement.

6.3 Right to an Accounting of Disclosures

You have the right to receive an accounting of certain disclosures of your PHI we have made in the six years prior to your request. This right does not apply to disclosures for treatment, payment, or health care operations; disclosures made to you; or disclosures made pursuant to an authorization.

6.4 Right to Request Restrictions

You have the right to request restrictions on our use and disclosure of your PHI for treatment, payment, or health care operations. We are not required to agree to all requested restrictions, except that we must agree to restrict disclosure to a health plan for payment or operations purposes if you have paid for the service in full out-of-pocket. If we agree to a restriction, we will honor it unless the PHI is needed to provide emergency treatment.

6.5 Right to Confidential Communications

You have the right to request that we communicate with you about your PHI by alternative means or at an alternative location. We will accommodate all reasonable requests. Please specify how or where you wish to be contacted.

6.6 Right to a Paper Copy of This Notice

You have the right to a paper copy of this Notice at any time, even if you have agreed to receive it electronically. You may also obtain a copy on our website at www.smartmedical.com.

6.7 Right to Notification of a Breach

You have the right to receive notification in the event that your unsecured PHI is breached. We will notify you without unreasonable delay and no later than 60 days after discovery of the breach, as required by the HITECH Act.

7. HOW WE PROTECT YOUR INFORMATION

Smart Medical has implemented comprehensive administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of your PHI, as required under the HIPAA Security Rule (45 CFR Part 164, Subparts A and C).

7.1 Administrative Safeguards

- Designated HIPAA Privacy Officer and Security Officer
- Mandatory workforce training on HIPAA privacy and security upon hire and annually thereafter
- Workforce access controls and authorization policies
- Regular risk analyses and risk management processes
- Sanction policies for workforce members who violate this policy
- Contingency planning and disaster recovery procedures

7.2 Physical Safeguards

- Restricted physical access to facilities where PHI is stored or processed
- Workstation use policies and screen locking requirements
- Secure disposal of paper and electronic PHI (shredding and electronic wiping/destruction)
- Visitor access controls and sign-in logs
- Equipment inventory and device tracking

7.3 Technical Safeguards

- Encryption of ePHI in transit (TLS 1.2 or higher) and at rest (AES-256)
- Unique user identification and multi-factor authentication (MFA)
- Automatic logoff and session timeout controls
- Audit logs and activity monitoring for all access to ePHI
- Firewalls, intrusion detection, and network segmentation
- Regular vulnerability assessments and penetration testing

8. BUSINESS ASSOCIATES

Smart Medical may share your PHI with third-party vendors and service providers (Business Associates) who perform functions on our behalf, such as billing companies, delivery contractors, IT service providers, accreditation organizations, and legal and accounting firms. We require all Business Associates to execute a Business Associate Agreement (BAA) that obligates them to:

- Use and disclose PHI only as permitted by the BAA and HIPAA
- Implement appropriate safeguards to protect PHI
- Report any known breach or security incident to Smart Medical
- Ensure their own subcontractors comply with equivalent HIPAA obligations

A current list of categories of Business Associates is available upon request from the Privacy Officer.

9. BREACH NOTIFICATION POLICY

Smart Medical maintains a comprehensive Breach Notification Policy consistent with 45 CFR Part 164, Subpart D. In the event of a breach of unsecured PHI, Smart Medical will:

- Conduct a prompt risk assessment to determine the probability that PHI has been compromised

- Notify affected individuals within 60 calendar days of discovery of the breach
- Notify the Secretary of HHS as required (annually for small breaches; within 60 days for breaches affecting 500 or more individuals)
- Notify prominent media outlets if a breach affects more than 500 residents of a state or jurisdiction
- Notify affected Business Associates as appropriate

Notifications will include a description of the breach, the types of PHI involved, steps you should take to protect yourself, steps Smart Medical is taking to investigate and mitigate the breach, and contact information for further questions.

10. SPECIAL CATEGORIES OF PROTECTED HEALTH INFORMATION

Certain categories of PHI are subject to heightened protections under federal and state law. Smart Medical applies additional safeguards to the following:

Category	Additional Protections
Mental Health & Substance Use Disorder Records	Subject to additional restrictions under 42 CFR Part 2 and applicable state law; may require separate authorization for disclosure.
HIV/AIDS Status	Disclosure may require specific consent under applicable state laws in addition to HIPAA authorization.
Genetic Information	Protected under GINA (Genetic Information Nondiscrimination Act); may not be used for underwriting purposes.
Pediatric PHI	PHI of minors is subject to additional state-specific protections and parental consent requirements.
State-Specific Protections	Some states impose stricter requirements than HIPAA; Smart Medical complies with the more protective standard in all applicable jurisdictions.

11. PRIVACY OFFICER AND CONTACT INFORMATION

Smart Medical has designated a HIPAA Privacy Officer and a HIPAA Security Officer responsible for developing and implementing our privacy and security policies and for receiving and processing complaints. You may contact our Privacy Officer with any questions, complaints, or requests to exercise your rights:

HIPAA Privacy Officer — Smart Medical
Mailing Address: Smart Medical, Attn: Audrey Ellis, Chief of Operations, at (610) 644-1370 or aellis@SmartMedicalcares.com
Email: privacy@smartmedical.com

11.1 Right to File a Complaint

If you believe your privacy rights have been violated, you have the right to file a complaint with Smart Medical or directly with the U.S. Department of Health and Human Services, Office for Civil Rights (OCR):

- U.S. Department of Health and Human Services, Office for Civil Rights, 200 Independence Avenue, S.W., Washington, D.C. 20201
- OCR Complaint Portal: https://www.hhs.gov/ocr/privacy/hipaa/complaints/

- Phone: 1-800-368-1019 (TDD: 1-800-537-7697)

Smart Medical will not retaliate against you for filing a complaint in good faith.

12. WORKFORCE COMPLIANCE AND ENFORCEMENT

Smart Medical's commitment to HIPAA compliance includes:

12.1 Training Requirements

All workforce members, including employees, contractors, and volunteers, are required to complete HIPAA privacy and security training upon hire and at least annually thereafter. Training records are maintained for a minimum of six years.

12.2 Sanctions

Any workforce member who violates this policy or applicable HIPAA regulations is subject to disciplinary action, up to and including termination of employment or contract, and may be subject to civil and criminal penalties imposed by law. Violations must be reported immediately to the Privacy Officer.

12.3 No Retaliation

Smart Medical strictly prohibits retaliation against any workforce member or patient who in good faith: exercises their rights under HIPAA; files a complaint with the Privacy Officer or HHS OCR; participates in a HIPAA investigation; or opposes any practice they reasonably believe violates HIPAA.

12.4 Policy Review and Updates

This policy will be reviewed at least annually and updated as necessary to reflect changes in law, regulations, business practices, or the threat environment. Material changes will be communicated to all affected workforce members and patients.

13. RECORD RETENTION

Smart Medical retains PHI and HIPAA-related documentation as follows, in compliance with applicable federal and state requirements:

- Patient records (PHI): Minimum of 7 years from the date of last service, or longer as required by state law
- HIPAA policies and procedures: 6 years from creation or effective date, whichever is later
- Business Associate Agreements: 6 years from expiration or termination
- Breach risk assessments and notifications: 6 years
- Training records: 6 years
- Authorizations and requests to exercise rights: 6 years

All records are stored securely and disposed of in accordance with applicable destruction standards (shredding for paper; certified electronic destruction for digital media).

14. CHANGES TO THIS NOTICE

Smart Medical reserves the right to change this Notice and our privacy practices at any time, provided that such changes are permitted by applicable law. We reserve the right to make the revised or changed Notice

effective for PHI we already hold as well as any PHI we receive in the future. When we make a material change, we will:

- Post the revised Notice prominently on our website at www.smartmedical.com
- Make the revised Notice available at our facilities
- Provide a copy to you upon request

The effective date of the current version of this Notice is stated at the top of this document.

ACKNOWLEDGMENT OF RECEIPT

By signing below, you acknowledge that you have received a copy of Smart Medical's Notice of Privacy Practices and HIPAA Compliance Policy Statement. You are not required to sign this acknowledgment to receive services; however, your signature helps us document our compliance efforts.

Patient / Authorized Representative Signature		Date
Printed Name		Relationship to Patient (if applicable)

Smart Medical — Protecting Your Health. Protecting Your Privacy.
www.smartmedgroup.com | privacy@smartmedical.com