ePHI Security & HIPAA Compliance Guide Sheet

MedForward Forms Online Service

Overview

HIPAA compliance is essential for any organization handling electronic medical information, and it is critically important for MedForward's clients receiving electronic patient information over the internet to understand what HIPAA requires, how MedForward complies with applicable regulations, and which tools MedForward provides to support your organization's own compliance obligations. You will be asked to sign a business associate agreement (BAA) with MedForward.

MedForward employs a layered suite of safeguards to enable your organization to remain HIPAA compliant when receiving electronic communications through your website with the MedForward Forms online service. All data is protected with TLS encryption in transit and AES-256 encryption at rest, all user accounts require multi-factor authentication by default, all access is fully audited, data is backed up daily to an off-site location, and the hosting datacenter is independently attested and monitored around the clock.

MedForward defines electronic protected health information (ePHI) in the context of the MedForward Forms toolkit as any information provided by internet users onto the pre-specified, secured, configured web forms that passes through or is stored on MedForward servers.

Administrative Safeguards — 45 CFR § 164.308

§ 164.308(a)(1) — Security Management Process

"Implement policies and procedures to prevent, detect, contain, and correct security violations."

MedForward conducts periodic security risk assessments of its systems, applications, and operational processes, and remediates identified risks under the oversight of its designated Security Officer. Systems are patched and scanned for vulnerabilities on a regular basis, and every software update undergoes a security and functionality review on a preproduction server before being deployed to the live production environment.

§ 164.308(a)(2) — Assigned Security Responsibility

"Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate."

Michael Weiss serves as MedForward's designated Security Officer, responsible for the development, implementation, and oversight of MedForward's security policies and procedures.

§ 164.308(a)(5) — Security Awareness and Training

"Implement a security awareness and training program for all members of its workforce (including management)."

All MedForward employees undergo background checks, sign confidentiality agreements, and complete HIPAA training annually. MedForward also provides training in the use of the secure back-end software to client organizations as part of all configuration projects. User accounts are created only upon request by a pre-designated authorized contact within the

client organization, and MedForward's user deployment process ensures that only the individual user — not administrators — knows their own credentials.

§ 164.308(a)(6) — Security Incident Procedures

"Implement policies and procedures to address security incidents."

MedForward maintains a documented security incident response protocol. In the event of a suspected or confirmed breach of unsecured ePHI, MedForward preserves relevant evidence and audit records, investigates and contains the incident, and notifies affected clients without unreasonable delay and in no case later than 60 calendar days after discovery, consistent with the Breach Notification Rule (45 CFR § 164.410), providing the information clients need to satisfy their own notification obligations.

§ 164.308(a)(7) — Contingency Plan

"Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information."

All data is backed up daily to a secure off-site location hosted on Rackspace infrastructure and covered under the same business associate agreement as MedForward's production systems. In the event of a hardware failure or other emergency, MedForward maintains a conservative service restoration target of 24 hours. Restoration from backup is periodically tested, with the most recent successful test restore completed in April 2026.

§ 164.308(b) — Business Associate Contracts and Other Arrangements

"A covered entity may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances … that the business associate will appropriately safeguard the information."

MedForward executes a business associate agreement with each client organization. MedForward likewise maintains a business associate agreement with its datacenter hosting provider, as required for subcontractors under § 164.308(b)(2) and the HIPAA Omnibus Rule.

Physical Safeguards — 45 CFR § 164.310

§ 164.310(d)(2)(i) — Device and Media Disposal

"Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored."

Data retention periods are configurable on a per-client basis upon request. By default, submitted data is retained for the life of the client account. Upon account cancellation, data is purged from MedForward servers only after the client confirms that all relevant records have been downloaded to satisfy the client's own record-retention obligations. ePHI will also be deleted and purged upon authenticated client request. MedForward requires validation of client identity through phone verification, including known details about the account, before purging any data. Clients remain responsible for complying with applicable state and federal medical record retention requirements.

§ 164.310(d)(2)(iv) — Data Backup and Storage

"Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment."

No equipment that stores ePHI is moved. Nonetheless, complete off-site backups of all data are performed daily.

Datacenter Security

Physical safeguards for the facility housing systems that contain ePHI.

MedForward's production systems are hosted on dedicated physical server infrastructure in a Rackspace datacenter in Chicago, Illinois, with 24-hour monitoring, controlled physical access, and on-site security. The datacenter provider maintains independent SOC attestations covering physical security, environmental controls, and operational processes.

Technical Safeguards — 45 CFR § 164.312

§ 164.312(a)(2)(i) — Unique User Identification

"Assign a unique name and/or number for identifying and tracking user identity."

Each user accessing the system is assigned a unique username specific to the identity of the employee or individual with access. Shared logins are prohibited.

§ 164.312(a)(2)(ii) — Emergency Access Procedure

"Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency."

MedForward Forms is available from any internet location. ePHI is recoverable only through a secured back-end portal protected by an encrypted TLS connection, with daily off-site backups available for restoration in an emergency.

§ 164.312(a)(2)(iii) — Automatic Logoff

"Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity."

Web forms containing patient data become inactive after ninety minutes of inactivity by default; the back-end administrative portal forces a logout after forty-five minutes of inactivity. Session timeout values can be adjusted to meet a client organization's policies. Separately, patients may save an in-progress form submission and resume it later using a unique server-generated access code delivered by email; resuming requires the patient to match multiple identity fields — name, date of birth, address, email address, and phone number — before the saved submission is restored.

§ 164.312(a)(2)(iv) — Encryption and Decryption

"Implement a mechanism to encrypt and decrypt electronic protected health information."

All communication between users and MedForward's servers is sent over TLS-encrypted connections. Data at rest is encrypted using AES-256, with additional column-level encryption applied within the database.

§ 164.312(b) — Audit Controls

"Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information."

All activity on the secured back-end portal is tracked and recorded in a comprehensive audit log, which is retained indefinitely. Users with administrator, developer, or auditor privileges can view and search this log.

§ 164.312(c)(1) — Integrity

"Implement policies and procedures to protect electronic protected health information from improper alteration or destruction."

In addition to requiring authenticated access over encrypted connections, submitted ePHI cannot be altered, deleted, or destroyed by users without first contacting MedForward. Standard access only allows data to be marked as archived and hidden from typical views; archived data can be recovered by authenticated users through search functionality. MedForward requires validation of client identity through phone verification, including known details about the account, before purging any data.

§ 164.312(d) — Person or Entity Authentication

"Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed."

All users must provide valid authentication credentials to access ePHI. Passwords must be at least twelve characters long and contain a mix of uppercase and lowercase letters, numbers, and special characters, and multi-factor authentication is enabled by default for all user accounts. Repeated incorrect login attempts result in user lockout, and MedForward requires validation of client identity through phone verification, including known details about the account, before unlocking users.

§ 164.312(e)(2)(i) — Integrity Controls

"Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of."

All data is transmitted solely over verified, TLS-encrypted connections, protecting ePHI against interception and undetected modification in transit.

§ 164.312(e)(2)(ii) — Encryption

"Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate."

All transmitted data is sent over secure, verified TLS-encrypted connections. The database is additionally encrypted at rest with AES-256 and at the column level, ensuring that datacenter personnel cannot access electronic protected health information.

PHI-Free Email Notifications

Preventing ePHI exposure through unsecured email channels.

Form-submission notification emails sent to client staff contain no patient data. They serve solely as alerts containing a link to the secured back-end portal, where full authentication is required before any submission can be viewed. Notification emails are delivered through MedForward's own email server hosted on its Rackspace infrastructure — no third-party email service handles system messages. The MedForward Forms system does not transmit ePHI over standard email.

HITECH Act & Omnibus Rule Obligations

The HITECH Act and the 2013 HIPAA Omnibus Final Rule make business associates such as MedForward directly responsible for safeguarding ePHI. MedForward meets these obligations as follows:

- Defining PHI: MedForward defines ePHI in the context of the MedForward Forms toolkit as any information provided by internet users onto the pre-specified, secured, configured web forms that passes through or is stored on MedForward servers.
- Backup and secure transmission: all information is backed up daily to an off-site location and transmitted exclusively over TLS-encrypted connections, with AES-256 encryption at rest.
- Access controls and tracking: MedForward Forms provides a comprehensive, indefinitely retained audit log of all actions taken by users in the system, covering both public-facing interfaces and back-end access.
- Uses and disclosures: while connected to the MedForward Forms system, all recovery of and access to ePHI is recorded.
- Authorized, trained personnel: user accounts are created only upon request by a pre-designated authorized contact within the client organization, training is provided as part of all configuration projects, and only individual users know their own credentials.
- Breach notification: MedForward maintains a documented breach response protocol under which evidence is preserved, incidents are investigated and contained, and affected clients are notified without unreasonable delay and no later than 60 days after discovery, enabling clients to meet their own obligations to notify individuals and the Department of Health and Human Services.

Looking Ahead: The HIPAA Security Rule Update

In January 2025, the HHS Office for Civil Rights published a proposed rule that would constitute the most significant update to the HIPAA Security Rule in more than two decades, with finalization targeted for 2026. The proposal would, among other changes, make multi-factor authentication and encryption mandatory rather than “addressable,” shorten incident notification timelines, and require regularly tested backup and recovery capabilities.

MedForward’s platform already reflects the direction of these changes: multi-factor authentication is enabled by default for all users, all data is encrypted in transit and at rest, backups run daily with a conservative 24-hour restoration target, and audit logs are retained indefinitely. MedForward is actively monitoring the rulemaking and is committed to full compliance within the compliance window once a final rule is published, so that our clients’ vendor documentation remains current as requirements evolve.

Data Privacy & Responsibilities of the Client

While MedForward works to secure all information on its platform, complete HIPAA compliance requires users and software to work together. If the software is not used properly — for example, if a user discloses their login credentials to a third party — confidential medical information may be exposed in violation of HIPAA. MedForward’s Terms and Conditions of Use require client organizations and their users to practice the following security measures:

- Log out immediately when stepping away from a machine.
- Never disclose a password to anyone, including someone claiming to be from MedForward. MedForward will never ask for your password.

- Never share a login with another person. It is critical that each person access MedForward Forms using their own unique username, password, and multi-factor authentication.
- Never share multi-factor authentication codes or approve authentication prompts you did not initiate.
- Use strong, unique passwords. A reputable password manager is recommended. Change your password immediately if you suspect it may have been compromised.
- Administrators must promptly remove the user accounts of employees who no longer work within their organization.
- Before logging in, verify that the URL clearly displays https and the domain name regularly used by your organization. MedForward cannot be held liable for organizations or individuals impersonating MedForward.
- Never share access to email accounts associated with your MedForward account, as these are used for account recovery and saved-submission access codes.

To protect the security of clients and their patients, MedForward reserves the right to close accounts or cancel the service of clients who appear to violate these terms and conditions.