MedForward Forms ePHI & HIPAA Compliance Guide Sheet

Document Last Reviewed: May 13th, 2014

Overview

HIPAA compliance is important for any company dealing with electronic medical information, and it is critically important for MedForward's clients that receive electronic patient information over the internet to know what HIPAA requires, how MedForward complies with regulations, and be aware of the tools that MedForward offers to enable your company to be compliant.

You will be asked to sign a business associate agreement with MedForward. MedForward employs a suite of safeguards to enable your organization to be HIPAA compliant when receiving electronic communications through your website with the MedForward Forms online service. With MedForward Forms, your forms are protected with SSL encryption and authentication. All access is fully audited. The system is backed up routinely and the datacenter meets specific stringent security and data integrity requirements. Through this suite of tools, the electronic protected health information (ePHI) is protected. 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.

HIPAA Compliance Provided By Virtue Of:

- ***Section 164.310(d)(2)(iv)*** *"Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment."*
    - No equipment that stores data is moved. Nonetheless, there are weekly off-site back-ups of all data.
- ***Section 164.310(d)(2)(i)*** *"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."*
    - ePHI will be deleted and purged upon request. Data older than five years may be marked for purgation, although client will be notified before this occurs and this can be configured on an individual basis.
- ***Section 164.312(a)(2)(i)*** *requires that you "Assign a unique username and/or number for identifying and tracking user identity."*
    - MedForward Forms addresses this by giving each user accessing the system a unique username specific to the identity of the employee or individual with access to the system.
- ***Section 164.312(a)(2)(ii)*** *"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 only recoverable through a back-end portal protected by SSL connection.
- ***Section 164.312(a)(2)(iii)*** *"Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity."*

    - Web forms containing patient data will become inactive after ninety minutes of inactivity. The back-end portal for administrative access forces a log out after forty-five minutes of inactivity.
- ***Section 164.312(a)(2)(iv)*** *"Implement a mechanism to encrypt and decrypt electronic protected health information."*
    - All communication between users and MedForward's server is sent over SSL encrypted connections. Data at rest is also encrypted.
- ***Section 164.312(b)*** *"Implement hardware, software and/or procedural mechanisms that record and examine activity in information systems that contain or user electronic protected health information."*
    - All activity on the secured back-end portal is tracked and recorded in a comprehensive audit log. Users with administrator, developer, or auditor privileges can view or search this log.
- ***Section 164.312(c)(1)*** *"Implement policies and procedures to protect electronic protected health information from improper alteration or destruction. Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner."*
    - In addition to requiring user authentication with password credentials over an SSL secure connection, submitted ePHI cannot be altered, deleted, or destroyed without first contacting MedForward. All access only allows data to be marked as archived and hidden from typical access. This data can be recovered by authenticated users using the search functionality. MedForward will require validation of client identity through phone verification, including known details about the client, before purging any data.
- ***Section 164.312(d)*** *"Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed."*
    - All users must provide correct authentication credentials to have access to ePHI, including a secure complex password, and an answer to a security question for access on new computers. Repeated incorrect attempts to log in will result in a user lockout. MedForward will require validation of client identity through phone verification, including known details about the client, before unlocking users.
- ***Section 164.312(e)(2)(i)*** *"Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network. Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of."*
    - All data is sent solely over secure SSL encrypted connection, which securely prevents interception of ePHI.
- ***Section 164.312(e)(2)(ii)*** *"Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate."*
    - When transmitted, all data is sent over secure verified SSL encrypted connections. SQL database database is also field encrypted to ensure datacenter staff cannot access the electronic protected health information.

The Feb 17, 2010 HITECH Additions to HIPAA specify the obligations of vendors providing secure services. MedForward complies as follows:

- *Know what information in your account is 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.
- *Make sure that information is backed up, transmitted securely, and encrypted if needed.*
    - All information is backed up weekly, and transmitted over a secure SSL encrypted connection.
- *Implement access controls to track who could have accessed that information — both from the public interfaces and through their back end systems.*
    - MedForward Forms provides a comprehensive audit log of all actions taken by users in the system.
- *Track uses and disclosures of that information.*
    - While connected to the MedForward Forms system, all recovery and access to ePHI is recorded.
- *Ensure that all staff that may be accessing your PHI in any way are trained and authorized.*
    - MedForward offers training in the use of the secure back-end software as part of all configuration projects. Additionally, users are only created upon request by a pre-designated authorized contact within the client organization. MedForward deploys an easy to use user deployment tool such that only individual users (not administrators) know their password and security question answers.
- *Report unauthorized disclosures of PHI to Health and Human Services and possibly the media.*
    - MedForward has specific breach protocol policies in place to purge compromised data and alert clients of all unauthorized disclosures detected.

Data Privacy & Responsibilities of Client.

While MedForward does its best to secure the information, if the customer does not properly use the software, confidential medical information may be disclosed, violating HIPAA. Complete HIPAA compliance requires both users and software to work together.

For example, if a user discloses his or her password or login information to a third party, it may allow a user to bypass security measures. It is critically important that all users practice the following security measures.

MedForward's Terms and Conditions of Use require customers to do the following:

- Logout immediately when walking away from a machine.

- Never disclose a password to anyone, including someone claiming to be from MedForward.
- Change your password at least every 90 days.
- Do not share login with another person. It is critical that each person access MedForward Forms using their own username and password.
- Administrators must delete the user accounts of employees who no longer work within their organization.
- Do not write down a password anywhere.
- Make sure that the URL clearly displays both **https** and the domain name regularly used when logging in. MedForward cannot be held liable for organizations or individuals impersonating MedForward.
- Never share access to e-mail accounts that are associated with your MedForward account.

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