



MedVirginia Statement on Privacy, Security, and HIPAA Compliance

As everyone in the healthcare industry is aware, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires covered entities to protect the privacy and security of protected health information (PHI). While MedVirginia is not a covered entity, it is a business associate of its client medical practices. It is through this business associate relationship with its clients that HIPAA becomes applicable to MedVirginia and *Solution*[®]. To fulfill its commitments as a business associate and recognizing that HIPAA compliance is of the utmost importance to its clients and the success of *Solution*, MedVirginia has implemented the following proactive, preventative privacy and security features:

- MedVirginia requires that all client medical practices (covered entities) enter into a Business Associate Agreement with MedVirginia (the business associate). This Agreement, which is incorporated into the standard MedVirginia *Solution* client agreement, outlines MedVirginia's responsibilities concerning the PHI contained in *Solution* and memorializes MedVirginia's commitment to HIPAA compliance.
- The central tenet of *Solution* is that a provider is able to render the best healthcare when the provider has access to all of a patient's health information. This core ideal has led MedVirginia to limit access to an individual's PHI to only those healthcare providers who have an established treatment relationship with that individual. Each user must sign a User Agreement in which the user agrees to only access an individual's PHI for treatment of that individual. Access is then technically limited by requiring a user to either declare a treatment relationship through *Solution* or establish a relationship through an interface with the provider's practice management system or upon receipt of test results or consult requests. Not only is it just good practice to ensure that only those providers with a bona fide treatment purpose view an individual's PHI, it is also important for HIPAA compliance. Under HIPAA, patient consent is not needed before a covered entity uses or discloses PHI for treatment purposes. Because clients and users who input PHI into *Solution* are sharing PHI for treatment purposes and those who access the information within it do so only when rendering patient care, MedVirginia has determined that use of *Solution* is HIPAA compliant without additional patient consent.
- MedVirginia recognizes that not all PHI is created equal. There are some types of PHI that are so sensitive that an additional layer of security is needed. Examples of such information include HIV test results, HIV status and the use of prescription medications that are exclusively used to treat HIV. These items, along with other highly sensitive information, will not be readily viewable in the standard electronic chart. Instead, the chart will contain a symbol that indicates the presence of highly sensitive information without disclosing any specifics. If the provider believes that knowledge of that highly sensitive information is critical to his ability to properly treat the patient, the provider can "break the glass" by declaring his reasons for viewing the sensitive information. In this way, *Solution* is ensuring that highly sensitive information is only viewed when absolutely necessary. Furthermore, *Solution* records each instance of "glass breaking" therefore deterring any improper use. (A more complete list of those items qualifying as highly sensitive is available upon request.)
- *Solution* complies not only with HIPAA, but also Virginia law under which there are two types of PHI that are more protected than all the rest: HIV test results and psychotherapy notes.



- HIV test results can only be disclosed to “[h]ealth care providers for purposes of consultation or providing care and treatment to the person who was the subject of the test or providing care and treatment to a child of a woman who, at the time of such child’s birth, was known to be infected with human immunodeficiency virus.” Va. Code. Ann. § 32.1-36.1(A)(4). Access to HIV test results through *Solution* will be compliant with this statute as a treatment relationship must exist between the provider and the patient before the provider can access the results. Additionally, HIV test results are a break the glass item; therefore, a user will have to declare that knowledge of the results is necessary to properly treat the patient.
- Pursuant to the Virginia Health Records Privacy Act (Va. Code. Ann. § 32.1-127.1:03), an individual’s psychotherapy notes cannot be disclosed without the written authorization of that individual. The Code defines “psychotherapy notes” as “comments, recorded in any medium by a healthcare provider who is a mental health professional, documenting or analyzing the contents of conversation during a private counseling session with an individual or a group, joint, or family counseling session that are separated from the rest of the individual’s health record.” Psychotherapy notes’ shall not include annotations relating to medication and prescription monitoring, counseling session start and stop times, treatment modalities and frequencies, clinical test results, or any summary of any symptoms, diagnosis, prognosis, functional status, treatment plan, or the individual’s progress to date.” MedVirginia is advising its clients that psychotherapy notes, as defined above, should not be shared through *Solution*.
- *Solution* is a subscription only service for healthcare providers. MedVirginia requires each client to provide information on its users to ensure that each user has the necessary credentials to access *Solution*. Once credentials are verified, each user is given a unique user identifier and password that is needed to logon to *Solution*. Because *Solution* employs a user identification password system, MedVirginia is able to audit individual user activity. Each user is assigned access rights based on role (e.g., physician, nurse, administrator). Each month and on an ad hoc basis, MedVirginia generates audit reports that detail the various ways in which users utilized *Solution*. For instance, MedVirginia is able to see the number of times any one user self-declared a relationship with a patient or a certain user “broke the glass”. MedVirginia has created numerous policies that outline the ways in which these audit reports will be examined to detect potential improper uses of *Solution* and the ways in which such potential problems will be investigated and remedied. (Copies of these policies are available upon request.)
- One of the main goals of *Solution* is to improve upon the status quo with respect to the sharing of PHI between providers for treatment purposes. To that end, MedVirginia believes that it has created a PHI sharing system that is more capable of protecting the privacy of PHI than the current paper record systems maintained in the majority of medical practices. For instance, in the current system, when one provider wants to share test results with another provider, that information is typically faxed to the second provider’s office. Any number of office staffers has access to that fax and there may be no record of who actually views it, reviews it or files it. In *Solution*, by contrast, the test results are sent directly to the provider’s inbox where only designated individuals have the ability to view it. Further, *Solution* has the ability to track each person who views, reviews and files the results. In this way, *Solution* offers far greater privacy protections than the current system for sharing PHI.



- Clients and users have the ability to transcribe office notes through *Solution*. While this information is very important to the dictating provider, it is not necessarily helpful to other providers who are treating the same patient. Recognizing this, MedVirginia has chosen to limit access to transcribed practice notes to only that user (and the associated client) who dictated them. The user can, of course, send a copy of the office note to another provider at any time through *Solution*'s secure messaging system.
- MedVirginia's systems are protected by CISCO ASA intrusion prevention devices. Partner access to MedVirginia's systems is secured by site-to-site IPSEC VPN tunnels. Partner access is restricted to the destinations and ports necessary for operation. Server security is accomplished through the combination of both network security (ASA) and at the machine level utilizing the software firewall built into the Linux operating system. Internal Security is accomplished through network segmentation that is implemented to provide isolation of the core application from other internal services. Access from other internal networks is limited to specific destinations and ports. User password requirements are based on password length, special characters required and periodic expiration of passwords. User access and all activity are audited throughout every touch point within the system.
- MedVirginia operations, interface systems and internal servers are housed at a highly secure Tier 3, SAS 70 enterprise-class data center in Richmond, VA.
- In addition to the various technical security mechanisms already discussed, *Solution* also contains the following security features:
- Access to MedVirginia *Solution* through a secure web portal
 - Use of a dedicated, secure server
 - Use of unique, alphanumeric user identifiers and passwords
 - Role-based access control
 - Automatic logout after 30 minutes
 - Inability to logon to *Solution* after three consecutive failed attempts
 - Ability to immediately deactivate a user identifier and password if improper use is suspected
 - Secure messaging to other *Solution* users
 - Inability to message non-*Solution* users