VieBridge, Inc.
Privacy and Security Policies for the e-CAP System

Please read these policies carefully before accessing or using the Service. Throughout this Policy Document, VieBridge, Inc. is referred to as "we" or "us."

1.0. Privacy Policies Related to You as a User

This portion of the Privacy and Security Policies describes how in the e-CAP system (hereinafter referred to as Service) we collect information from you or about you, why we collect this information, how we will use or disclose this information and how you can update or delete personably identifiable information collected about you from our records.

1.1. Use of Cookies

The Service is Web-based and, as such relies on the use of cookies. Cookies are bits of data that a web site can store into your computer browser to help VieBridge provide a satisfactory user experience along with also providing us usage data. The use of cookies is a standard practice among Internet websites. To better serve you, we occasionally use "session cookies" to enhance or customize your visit to this website. The cookie does not store any PHI (personal health information) or PII (personally identifying information) and they do not compromise any security or privacy. A session cookie is erased during operation of your browser or when your browser is closed. The use of cookies is required for effective use of the service. Disabling or deleting them may result in unpredictable results.

1.2. IP Addresses

There are several types of information we collect. For all visitors to the Service, we collect and log your IP address. An IP address is a number automatically assigned to your computer whenever you access the internet. IP addresses allow computers and servers to recognize and communicate with one another. We collect IP address information to properly administer our system and to gather aggregate information on visitors to our site and how our site is being used, including the pages visitors are viewing. This aggregate information is not shared with advertisers, sponsors and others businesses. To maintain your anonymity, we do not associate IP addresses with records containing personal information. We will use IP address information, however, to personally identify you in order to enforce our legal rights or when required to do so by law enforcement authorities.

1.3. Other Sites

Our privacy policies apply only to your use of the Service. The Service contains links to other sites, including sites that may indicate a special relationship with us. While we do not disclose personally identifiable information to those operating these linked sites, we are not responsible for the privacy practices of such other sites. You should read the privacy policies of each site you visit to determine what information that site may be collecting about you.

2.0. Security Policies and Requirements

The Service contains personal health information on individual beneficiaries. It is important that Medicaid beneficiary's personal information is protected, meaning it must be kept private and secure. As the referral, assessment and plan of care entity for the North Carolina Medicaid CAP program, VieBridge, Inc., is committed to maintaining the security and privacy of beneficiary's personal health information.

2.1. Federal Requirements

To ensure the privacy and security of beneficiary personal health information, VieBridge, Inc. is guided by key provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA). This legislation established national standards for electronic health care transactions and national identifiers for providers, health plans, and employers. Now that the federal government is mandating patient records be sent over digital networks, patient privacy is that much more a priority. Consequently, HIPAA law affects "systems that transmit health information in electronic form in connection with standard transactions".

2.2. Making Sure Beneficiary Information is Private and Secure – Service Security Measures

Data privacy entails controlling who is authorized to access Protected Health Information (PHI) of beneficiaries. Privacy and security measures must be implemented, such as the ability to control access to data, protect it from accidental or intentional disclosure to unauthorized persons, and guard it against unauthorized alteration, destruction, or loss.

To increase the security provided for electronically handled data, the Service is designed to ensure both confidentiality and security. The security measures built into the Service are summarized below. The Service is a web service. It is centrally hosted by VieBridge, Inc. The Service web service is made secure through these primary measures:

- The centralized hosting location is a secure, HIPAA-compliant facility.

- Access to the central hosting site is strictly controlled.

- The Service is configured as an https web site, which is a standard, generally recognized method for data security that is a combination of the Hypertext Transfer Protocol (HTTP) with the Secure Socket Layer/TLS protocol to provide encrypted communication and secure identification of the web server used by the Service.

- The Service is verified and certified as a trusted site by Network Solutions, an independent certificate authority.

- All beneficiary information is secured during transmittal across the Internet by use of encryption software that is used to encode information in such a way that only the computer connected to the Service.

- No beneficiary information is transmitted outside the secure transmittal method.

- Each user must be registered by VieBridge, Inc. or its designated representatives. (See details of registration below.)

- Each user must log in and be verified as a registered user.

- Each registered user’s access rights are governed by assignment to different groupings that determine what the user can do or see on the Service.

2.3. Service User Responsibilities for Data Security

While the Service is designed as a secure web service, each individual user is an important part of the overall security program. The most important purpose of security is to guarantee that beneficiary information is disclosed only to authorized individuals. Safeguards are needed to grant access only after the person requesting the information has been properly identified and authenticated. In the Service, only individuals registered by VieBridge, Inc. can access the Service. Below we describe four (4) steps to ensure beneficiary data security in your agency and operation.

Step 1. Have a Data Security Policy and Plan Make sure your agency creates, approves, and follows a data privacy policy and procedure that is specific to the purposes and operation of your agency. Make sure the plan is reviewed and adopted by each office of your agency.

Step 2. Control Registration of Users to the Service. Make sure your agency keeps track of who is currently authorized as a Service user. Follow these guidelines on registration and access:

- Any change in user access rights must be formally requested, in writing.

- Only designated agency staff can request changes in staff registrations for the Service.

- Report any staff who no longer works for your agency immediately. Failure to do so is a serious security breach.

- Register users by provider billing number. The Service information is organized around beneficiary MID and agency provider numbers. No registration will be accepted unless the proposed staff member is associated or assigned to the provider numbers(s) of your agency.

- Any organization or individual that is a designated representative of your agency must be authorized, in writing, by your agency as a Service user. Agencies can list designated representatives on the Service registration form. When doing so, identify which provider numbers the designated representative will be able to access via the Service.

Step 3. Protect Usernames and Passwords

Make sure your agency and staff follow these basic guidelines for usernames and passwords:

- Do not share usernames and passwords.

- Do not write down and leave passwords in public view.

- Change user passwords on a routine basis.

- Make sure passwords are not easy to guess or obviously associated with the user.

Step 4. Secure Computers

Secure the agency (or personal) computers that are used to connect to the Service. Take into account the following security capabilities and procedures:

- Have active and current anti-virus and malware detection software running on each computer used to access the Service.

- Individual users must log into the computer each time they use the computer.

- The log-in requires a password that contains sufficient letters and numbers to be difficult to guess.

- The computer should have a screensaver that activates within 5 minutes of non-use.

- The computer should log-off the user when the computer is inactive for more than 10 minutes.

- Computer screens should be positioned so that the contents of the screen cannot be viewed by persons walking by.

- Downloading and storing of beneficiary data on local computers is discouraged by not prohibited. The security of any beneficiary data downloaded to a local computer is the responsibility of the User's Agency – not VieBridge, Inc.

- If beneficiary data (like a request or an assessment) is printed out for reference and review by staff, make sure there is a cover page labeled Confidential that can be placed over any printout while the beneficiary information is placed on a desk or in a workspace.

- If the user is accessing the Service from a location other than an agency office, the same security and privacy provisions should be observed without exception.

- If the hardcopy of the beneficiary information obtained from the Service is added to a beneficiary chart or record, the agency must ensure that there are security measures and protocols in place to protect the charts/records from inappropriate access by unauthorized users.

- Provide periodic training of all permanent (and temporary staff) on privacy requirements and the procedures to be followed to assure data privacy.

2.4. Communicating Questions About Beneficiary-Specific Information

Do not transmit beneficiary information to anyone, including VieBridge, Inc., via unsecured email. If your agency has a question for VieBridge, Inc. about beneficiary specific information, do NOT send any unsecure email or on-line question via the Service with beneficiary specific information. VieBridge, Inc. supports the use of Zixmail as a secure email service. Zixmail cannot be used to communicate beneficiary information (or attachments with beneficiary information) unless your agency is an enrolled subscriber to Zixmail; however, you can reply to a Zix-encrypted email you receive. Use of the Service does not require your agency to enroll in Zixmail. If you have questions about how to set up and enforce data security of e-CAP beneficiary data, please contact the e-CAP Support Center and they will forward your question to the appropriate technical staff at (888) 705-0970.

3.0. Changes to Our Privacy and Security Policies

We may change the terms and conditions of our Privacy Policies at any time by posting revisions on the Service. You agree to review the Privacy Policies portions of this Agreement each time you use the Service so that you are aware of any modifications made to these policies. By accessing or using the

Service, you agree to be bound by all of the terms and conditions of the Agreement as posted on the Service at the time of your access or use, including the Privacy and Security Policies then in effect.