

## **Privacy Statement**

### **General Statement and Verification of Standards**

HealthHighway.com has adopted this privacy statement in order to demonstrate our firm commitment to Provider and Patient privacy. This Privacy Statement tells you how our company gathers information at this website. It also describes the protections we have in place for that information, and whether we disclose that information outside of this website, which is <http://www.HealthHighway.com/>.

### **Types of Information**

This web site handles three broad categories of information. Contact and demographic information, such as patient name, age and contact information, unique identifiers such as social security numbers or office medical ID numbers. Other types of information includes personally identifiable health information, and practice billing and financial information. The high level of security for each of these types of information is the same. We protect all Provider and patient data by encrypting it whenever that data is transmitted (see technical security below for details), and by requiring a series of user identification symbols, authentication techniques and passwords when the data is stored on the website.

### **Use of E-mail Address, Name and other Contact Information**

Our site's registration form asks you to give us contact information (such as name and email address), which we use to contact you when necessary and to identify you when you visit the web site. We do not provide make this information available to other entities, and we protect it from unauthorized use.

### **Use of Cookies and Internet Address**

We use "cookies", small temporary text files, placed on your computer in order to help you more easily navigate and use our web site. The cookies identify your computer during your visit so we can assist with your sessions on our web site and make the site and its features easier for you to use. Cookies also help us give you health information and other information that you might find interesting or helpful. The cookie files are temporary and expire each time you logout. We do not use cookies to save passwords. We may use your Internet address to diagnose problems with our server, administer our web site and assist with your web site sessions as described above.

### **Unique Identifiers**

Unique Identifiers (such as social security number or other unique identifying number) may be collected to verify your identity or for use as account numbers in our system.

### **Secure Electronic Messaging System**

Our secure electronic messaging for communications between providers and patients may be used only when both agree to use the system. We recommend that you discuss any questions your patients may have regarding the privacy of information that might be contained in the messaging system, should you and your patient(s) both decide to use it.

HealthHighway.com is not responsible for the privacy policies or practices of individual Provider's offices or their associations.

### Employees and Contractors

Each HealthHighway.com employee and independent contractor signs a Confidentiality and Privacy Agreement in which they agree to uphold the privacy policies and practices of HealthHighway.com

### Your have Right to Not to Participate in Portions of this Web Site

When you register for this website, you have a choice whether or not to participate in any or all of the services that we offer.

### Demographic Data and Opt-In Option for Receipt of Additional Information

When we ask you for demographic information during registration and at other points on the web site, the site allows you to choose whether or not to receive any online or mail communications from ProvidersAccess.com or its partners. You will not receive any unsolicited information without your consent.

### Third Party Disclaimer

Although HealthHighway.com makes every effort to seek out and associate with companies who respect your privacy as much as we do, we do not control and therefore cannot be responsible for the privacy policy or practices of any third party whose links and/or content may be found within the HealthHighway.com web site. If you are concerned about or interested in the privacy practices or policies of these other web sites, you may wish to review the statements posted on their web sites and/ or contact them directly with your questions.

### Advertisement and Sponsorship

Certain companies and their products sponsor the HealthHighway websites. The accuracy and use of the information provided by them including their product and services is your responsibility. If you are concerned about or interested in the privacy practices or policies of these other vendors, you may wish to review the statements posted on their web sites and or contact them directly with your questions.

Contacting HealthHighway.com If you have questions regarding this privacy statement or the practices of this web site you can contact us by e-mail at: [support@HealthHighway.com](mailto:support@HealthHighway.com).



---

## Technical Security Policy

### Introduction

As an application service provider facilitating communications between patients, provider offices and their associations, as an enterprise that maintains individually identifiable health information on behalf of these parties, and as a company dependent on health care transaction revenues for a significant portion of its income, HealthHighway.com (the Company) has a vital stake in ensuring the highest level of data security and confidentiality on behalf of its constituent users. For one thing, it will soon be mandated in regulations from the US Department of Health and Human Services (DHHS); criminal penalties will be exacted for knowingly and inappropriately releasing individually identifiable health information. For another, knowing how important confidentiality is to Provider-patient relationships, it simply is good business for Company employees to act as trustworthy stewards of this data.

On the other hand, there will never be perfect data security; malicious or inadvertent confidentiality breaches will occur. However, companies at least must be diligent in protecting confidentiality and in maintaining data security to the greatest practical extent. And when breaches inevitably occur, companies must actively monitor its systems to detect them, must take corrective action as quickly as possible upon detection, and must continually adjust its security and confidentiality policies and procedures to insure that they remain adequate. All of this is recognized implicitly or explicitly in the proposed rules on privacy that have resulted from the original HIPAA legislation from DHHS.

### Present Measures

The Company has NEVER planned nor suggested to customers that it would be advisable to eliminate paper records from its customer's practices. In fact, the Company has always regarded the data it collects and maintains on behalf of its users to be supplemental to medical care processes. Its operating model has been to function as an "electronic shadow chart" - recording information maintained for the convenience and improved efficiency of the Providers and other health care providers that use the system; as with other shadow charts; the final arbiter of, and source of documentation about, patient care remains the main (paper) chart

Nevertheless, the Company has put in place a number of measures to assure the security of its users data. First, data is hosted at the co-location facility (COLO) of an Internet Service Provider (ISP). The COLO is monitored 24-hours per day by ISP personnel, and the hosted systems are monitored continuously by ISP systems to detect a variety of possible attacks. The Company is notified by pager of any suspected security breaches.

The computers on which customer data is located are behind several sets of locked doors at the air-conditioned COLO. The COLO has 24 hour a day security, and policies and procedures are in place to log all entry and access to the computers containing customer data. ISP electrical power is carefully conditioned, and there is on line battery and automatic start generator backup of this power sufficient to cover 24 hours with no intervention, and indefinitely with refueling.

The Company has automatic tape-backup units for all computers containing customer data. Backup tapes are made at least nightly and stored in locked vaults that only selected Company employees can access.

Beyond that, the Company designed its systems to be compliant with National Research Council Guidelines developed to protect health information, published by the US National Academy of Science in 1997. In particular, all data interchange through company applications is encrypted (currently using up to strong domestic triple-DES 56-bit encryption via SSL where supported by client browser). Data access is protected by a system of User IDs and passwords. All updates to data are accompanied by audit information stored with it that records (among other things) date, time, user, nature of the change, and optional user comments. Finally, the system has an office-administrator-definable time-out, which upon expiration requires re-authentication of the user before further data access is allowed.

In addition, the Company protects its customers' (and its own) data using a state-of-the-art, market leading firewall, with a strict security policy. Additionally, strong encryption VPNs, and industry standard access controls are used to safeguard the privacy and availability of customer information

The Company is planning to perform regular internal security assessments, and periodic external audits by industry leading information security companies.

### Future Measures

The most important aspect of the proposed HIPAA regulations is the following: any organization that plans to exchange individually identifiable health information electronically with another individual or organization can only do so when appropriate "chain-of-trust" agreements are in place between these organizations or individuals.

Specifically, this means that these entities must themselves have an explicitly set of policies assuring some level-of-protection of this data, that there is effective administrative enforcement of these policies, and that there is continuous monitoring of the policies and their enforcement to insure that protection endures and improves over time to meet any threats.

Of course, the requirements for entering into chain-of trust agreements apply to the Company itself. HIPAA has a proposed two-year phase-in period before compliance is required. During that time, the Company must:

- a. Hire or designate a Chief Security Officer to assume responsibility for the Company's security measures.
- b. Have in place specific policies and procedures for ensuring adequate security and privacy protections; fully document this activity.
- c. Have in place adequate monitoring procedures to detect security breaches in a timely manner, and to assure that corrective measures are instituted as quickly as possible; fully document this activity.
- d. Upgrade technical security and privacy protections as needed to keep up with technical requirements; fully document this activity.
- e. Formally engage the Company's data interchange partners with chain-of-trust agreements based on the above; fully document this activity.

The Company has recently engaged a data security firm to begin conducting tests of its security and confidentiality protections. Testing protections against external attack is underway; testing against internal attack will occur shortly. A formal security audit by an accounting firm will be conducted before the end of June; results of this testing and of the audit will be posted on the Company web-site by that time.

The requirement for entering into chain-of-trust agreements applies equally to small-office Providers (Providers in practices of 10 or fewer providers - including solo practitioners). The Company is uniquely positioned to make it feasible for this constituency to enter into these chain-of-trust agreements.

The Company plans to offer to its office users a system of templates and reminders that will assist them in becoming and remaining HIPAA-compliant. In particular (almost exactly parallel to what the Company itself must do), it will implement a system that:

- a. Helps assign a party responsible for office security; documents this activity.
- b. Creates and periodically updates policies and procedures for ensuring adequate security and privacy protections; documents this activity
- c. Monitors and reports possible security breaches to these offices as soon as they occur; recommends corrective measures; documents this activity
- d. Continuously updates its own technical security and privacy protections (on behalf of its office and consumer users); documents this activity.
- e. Creates and submits to data interchange partners chain-of-trust agreements based on the above; fully documents this activity. The Company is committed to providing users with the information necessary to stay ahead of industry regulations, and keep their medical data secure.