Secure Health Information Technology Corp.
SecureHIT
Privacy Policy

Secure Health Information Technology Corp. a corporation duly organized and existing pursuant to the laws of the Commonwealth of Puerto Rico (hereinafter referred to as "SecureHIT", "we", or "us") respects and values your privacy. We will not knowingly use or share your personal information collected on this website and our related websites (collectively, the "Website") or provided through a Service except as described in this Privacy Policy. By using the Website or subscribing to or using a product or service described on the Website (each, a "Service"), you accept and agree to the privacy practices contained in this Privacy Policy. We encourage you to read this Privacy Policy in full to understand our privacy practices before using the Website, subscribing to a Service or submitting any personal information.

PLEASE NOTE THAT THIS PRIVACY POLICY MAY BE CHANGED FROM TIME TO TIME. We indicate at the top of the page when this privacy policy was last updated from time to time, we would like to contact you to Provide Service and Website related notices; Communicate with you regarding updates to the Service and Website; and to respond to your inquiries, requests and applications. If you consent to us contacting you for this purpose.

Information System Security Officer
We have appointed an information system security officer who is responsible for overseeing questions in relation to this Privacy Policy. If you have questions about this Privacy Policy or the Information System Security Officer at isso@securehitpr.com, or at: Information System Security Officer PO Box 1666, Sabana Seca, PR, 00952, U.S.A. If you are a citizen of the European Union, you have the right to make a complaint at any time to the supervisory authority or authorities for data protection issues in your country. We would appreciate the chance to deal with your concerns before you approach the data protection supervisory authorities, so please contact us at isso@securehitpr.com in the first instance.

Third Party Websites
Plug-ins and Applications. The Website or a Service may include links to third-party websites, plug-ins and applications. Clicking on those links or enabling those connections may allow third parties to collect or share data about you. We do not control these links, plug-ins or applications and we are not responsible for the practices employed by them and cannot accept responsibility for any use of your personal information by them. We cannot guarantee that they will adhere to the same privacy and security practices as us. If you click on those links or enable those connections, we encourage you to read their privacy policies before you submit any personal information. Your use of any such resource is at your discretion and at your sole risk.

Personal Information We Collect
Personal Information means information about an individual from which that person can be identified. It does not include information or data where the identity has been removed, or anonymous data.

When you create and account or subscribe to a Service, you will be asked to submit some or all of the following personal information to verify your identity and establish an account:

Name, home or other physical address, email address, phone number, social security number, fax number date of birth and npi number. For Organization Certificates, the applying entity will also be required to provide its name, EIN number, npi number, address, u.r.l. to which the Organizational Certificate is to be issued, and the name of an administrator for such organization, including the administrator's name, physical address, email address, phone number and fax number. This information is used by SecureHIT to verify your identity and for purposes of completing your registration process and creating an account.

A Service may also allow you to securely exchange protected health information as described in Section 5 below. If you create a .domain registration account, you will be required to provide (a) the registrant or legal owner of the domain, (b) an administrative contact responsible for matters regarding maintenance and servicing of the domain, (c) a technical contact, and (d) billing contact. For each of the foregoing, we collect the legal or organizational name, street address, phone number, fax number and email address.

We also collect, use and share aggregated data such as statistical or demographic data for any purpose. Such aggregated data does not directly or indirectly reveal your identity. However, if we combine or connect aggregated data with your personal information so that it can directly or indirectly identify you, we treat the

combined data as personal data to be used in accordance with this Privacy Policy. We do not collect any special categories of personal data that include details about your race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions, or trade union membership, information. Nor do we collect any information about criminal convictions and offenses.

If you fail to provide personal data where we need to collect personal data by law, or under the terms of a contract we have with you and you fail to provide that data when requested, we may not be able to perform the contract we have or are trying to enter into with you (for example, to provide you with a Service). In this case, we may have to cancel the Service you have with us, but we will notify you if this is the case at the time.

Procedure Used to Collect Information
We use various methods and technologies to collect personal information about visitors to the Website and subscribers to or users of the Service. These methods and technologies include the following:

Direct Interactions
You may give us your identity, contact and financial data by filling in forms or by corresponding with us by post, phone, email or otherwise. This includes personal data you provide when you:

- Subscribe to a Service;
- Create an account on the Website;
- Submit a support request;

SecureHIT on the Web
As is true of most websites, we gather certain information automatically and store it in log files. This information may include IP addresses, browser type, Internet service provider, operating system, date/time stamp and/or clickstream data. We or our marketing partners, on our behalf, may link this automatically collected data to other information we or they collect about you.

Cookies and other tracking technologies
We and our service providers may use technologies such as: cookies, beacons, tags and scripts. These technologies are used in analyzing trends, remembering users' settings, administering the Website and Service, tracking users' movements around the Website and Service and to gather demographic information about our user base as a whole. We may receive reports based on the use of these technologies by these companies on an individual as well as aggregated basis. You may control the use of cookies through your browser settings. If you reject cookies, you may still be able to use our Website, but your ability to use some features or areas of our Website, as well as use of the Service, may be limited.

Security and Health Insurance Portability and Accountability Act ("HIPAA")
SecureHIT and/or its third-party service providers have implemented reasonable security measures as required by HIPAA designed to protect against the loss, misuse or alteration of your protected health information transmitted through or stored by the Service. As a subscriber to the Service, you will also be able to send, receive and transmit protected health information with healthcare providers and other persons who have a Direct Certificate or have otherwise implemented a trusted relationship with the subscriber for the exchange of protected health information using the Service. However, please be aware that no data transmission over the Internet can be guaranteed to be 100% secure and this is not a guarantee that your personal information (including protected health information) may not be accessed, disclosed, altered or destroyed by breach of any physical and technical safeguards in place. All information you transmit on or through the Website and Service is at your sole risk. You are responsible for maintaining the secrecy of your unique password(s) and account information, and for controlling access to your account(s) at all times.

How We Use the Personal Information Collected
We may use your personal information collected for the following purposes: To create your Website or Service Account and allow the use of the Service. To better understand how the Service and Website are being used and to improve the Service and Website. To provide personalized Website and/or Service content based on your activity and preferences. To communicate with you regarding updates to the Service and Website and to respond to your inquiries, requests and applications and/or to send important notices. To conduct surveys and research. To track your use of the Website and Service as reasonably necessary to prevent illegal activities and enforce our Direct SecureHIT Agreement. We may also send you emails with information about SecureHIT products and services that we believe may be of interest to you. If you wish to opt-out of receiving these emails from us, please follow the instructions contained in that email.

How We Share Personal Information Collected

We do not sell or rent personal information or protected health information we collect through the Website or Service to any third party for its own marketing purposes. We will get your express consent before we share your personal information with a third party for their own marketing purposes.

We may share your personal information and protected health information as follows:

- We may disclose your personal information and protected health information to our Service Providers who provide certain services to us or on our behalf, such as operating, providing and supporting the Service, analyzing data, verifying your identity, processing payments or consulting services.
- These Service Providers will only have access to the personal information or protected health information needed to perform these functions on our behalf. Our Website may offer a publicly accessible blog. You should be aware that any personal information you provide in these areas may be read, collected and used by others who access them. To request removal of personal information from our blog or community forum, contact us at isso@securehitpr.com
- We may also disclose personal information about visitors to our Website or users of the Service:
    - As required by law, such as to comply with a subpoena or similar legal process.
    - When we believe in good faith that disclosure is necessary to protect our rights or property, protect your health and safety or the health and safety of others, or to investigate illegal activity or fraud or to respond to a government request.
    - In the event of a merger, acquisition, asset sale or in the unlikely event of bankruptcy, personal information (and protected health information) maintained by or on behalf of SecureHIT may be transferred to its successors or assigns.
    - To any other third party with your prior consent.
    - We may also share information relating to users of the Website or Service with affiliated or unaffiliated third parties on an anonymous, aggregate basis. While this information will not identify you personally, in some instances these third parties may be able to combine this aggregate information with other data they have about you, or that they receive from third parties, in a manner that allows them to identify you personally.

Children's Privacy

Children under the age of 18 are not permitted to create an account or use the Service, and we do not knowingly collect personal information from children under 13 years of age, except personal information and protected health information sent, received, transmitted or stored through the Service by a parent or legal guardian who is authorized to do so. If you believe that we may have improperly collected any information from or about a child under the age of 13, please contact us at isso@securehitpr.com

Special Notice for Users Located Outside the United States

The Website and Service are currently provided from the United State for use by persons in the United States. If you chose to access the Website or Service from any jurisdiction outside the United States, any personal information that we collect from you may be transferred to and stored at a destination outside of your country of residence, including the United States. By using the Website or subscribing to a Service, you hereby consent to the collection, transfer, storage, processing, and other use of your information in the United States or another destination outside of your country of residence. You acknowledge that your personal information may be subject to the privacy and data protection laws and regulations of the United States, which may not be the same as applicable laws and regulations in your country of residence.

Accessing, Changing and Managing Your Personal Information

The Website and/or Service may allow you to directly view, edit or delete personal information about you online. If this option is not available, you can update your personal information by contacting our Information System Security Officer at isso@securehitpr.com or the address or phone number listed above. We will use commercially reasonable efforts to respond to your request within 30 days.

Data Security

We have put in place appropriate security measures designed to prevent your personal data from being accidentally lost, used or accessed in an unauthorized way, altered or disclosed. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal data to perform services on your behalf and they are subject to a duty of confidentiality. We have put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator of a breach where we are legally required to do so.

Data Retention

We will only retain your personal data for as long as necessary to fulfil the purposes we collected it for, including without limitation, for the purposes of satisfying any legal, accounting, or reporting requirements.

To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorized use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

By law, we have to keep basic information about our customers (including contact, identity, financial and transaction Data) for six years after they cease being customers for tax purposes. For legal and audit purposes, we currently keep log data for up to six (6) years.

Your Legal Rights
Under certain circumstances, you have rights under the data protection laws in relation to your personal data. Please read below to find out more about these rights:

- Request access to your personal information. You may request a copy of the personal information we retain.
- Request correction of your personal information. You may correct any personal information we retain about you if it is incorrect or incomplete.
- Request erasure of your personal information. You may ask us to delete your personal information if there is no good reason for us to continue to retain it. You also may ask us to delete personal information in instances where (a) if you have successfully exercised your right to object to our processing of such personal information, (b) if we processed or are processing such personal information in violation of applicable law, or (c) if we are required to erase your personal information by law. However, we may not always be able to comply with your request due to legal or technological reasons. If this is the case, we will notify you at the time you request deletion of your personal information.
- Object to the processing of your personal information. You may object to our processing of your personal information if we are using it for marketing purposes, and, in instances where we are relying upon our or a third party's interests to process your personal information, if you believe it impacts your fundamental rights or freedoms.
- Request restriction of processing of your personal information. You may request that we suspended processing of your personal information if (a) you need it to defend, establish or exercise legal claims, (b) we need to verify our legitimate right to use your personal information in an instance where you have requested we stop processing it, (c) our processing of such personal information is unlawful but you do not want us to erase it, or (d) you want us to establish the personal information's accuracy.
- Request transfer of your personal information. If you request us to transfer personal information you provide to us in automated information or to perform a contract with you, we will use commercially reasonable efforts to provide this information to a third party in a machine-readable format.
- Right to withdraw consent. You have the right to withdraw your consent to our processing of your personal information if we are relying upon your consent to process such information. This will not affect any processing of such personal information before you withdraw your consent. If you withdraw your consent, we may not be able to provide you with a product or service for which you have subscribed. If this is the case, we will notify you at the time you withdraw your consent.

As mentioned by the federal requirement under the HIPAA law, SecureHIT is committed to complying with the following statutes;

§164.502(j)(1) Disclosures by whistleblowers: A covered entity is not considered to have violated the requirements of this subpart if a member of its workforce or a business associate disclose protected health information, provided that:
(i) The workforce member or business associate believes in good faith that the covered entity has engaged in conduct that is unlawful or otherwise violates professional or clinical standards, or that the care, services, or conditions provided by the covered entity potentially endangers one or more patients, workers, or the public; and
(ii) The disclosure is to:
(A) A health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of the covered entity or to an appropriate health care accreditation organization for the purpose of reporting the allegation of failure to meet professional standards or misconduct by the covered entity; or
(B) An attorney retained by or on behalf of the workforce member or business associate for the purpose of determining the legal options of the workforce member or business associate with regard to the conduct described in paragraph (j)(1)(i) of this section.

If you wish to exercise any of the rights set out above, please contact us at isso@securehitpr.com or you can inform us anonymously by writing us to PO Box 1666 Sabana Seca PR 00952.

NO FEE USUALLY REQUIRED
You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. Alternatively, we may refuse to comply with your request in these circumstances.

WHAT WE MAY NEED FROM YOU We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

TIME LIMIT TO RESPOND
We try to respond to all legitimate requests within one month. Occasionally it may take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

Changes to Privacy Policy
We will notify you of changes to this Privacy Policy by posting the amended terms on our Website at least thirty (30) days before the effective date of the changes. If you have provided us with your email address, we will also notify you of material changes to this Privacy Policy by sending an email at least thirty (30) days before the effective date of the changes to the email address you most recently provided to us. We encourage you to keep the email address you provide to us current, and to promptly notify us of any changes to your email address, so that you may receive any notices we send to you regarding material changes to this Privacy Policy.