HIPAA POLICY

The Health Insurance Portability and Accountability Act (HIPAA) was enacted by the U.S. Congress in 1996. HIPAA is also known as the Kennedy-Kirshenbaum Health Insurance Portability and Accountability Act (HIPAA-Public Law 104-191), effective August 21, 1996.

The basic idea of HIPAA is that an individual who is a subject of individually identifiable health information should have:
1. Established procedures for the exercise of individual health information privacy rights.
2. The use and disclosure of individual health information should be authorized or required.

One difficulty with HIPAA is that there must be a mechanism to authenticate the patient who demands access to his/her data. As a result, medical facilities typically request a social security number from patients, thus arguably decreasing privacy by simplifying the act of correlating health records with other records. The issue of consent is problematic under HIPAA, because the medical providers simply make care contingent upon agreeing to the privacy standards in practice.

How we attempt to solve this dilemma is through encrypted Wallets. Because you must have a profile and a wallet to access our platform, your identification is secured as a Wallet Address ID, thus requiring keys to access information. Only you have access to your keys. Keys for records sharing with Doctors/Providers will also be performed. Also since we are cryptocurrency cash based method of payment for care, there is no need for credit, debtor notes, no insurance filings. If you however, need these systems above and beyond CPX to pay for a service, this will take place OFF PLATFORM.

Who has access to my Personally Identifiable Information?
Only authorized and verified Doctors and/or Providers who utilize our Blockchain network may access your information to administer services requested by you. All of the authorized healthcare Doctors/Providers must sign an agreement to follow the network's Policies that includes a nondisclosure and confidentiality agreement. All Doctors/Providers must undergo KYC verification which includes photos, identification, business license, medical license, and checking with other third party registry or databases to verify their identity.

We may work with other 3rd parties to help us conduct our business. We are required by law to sign an agreement with these external companies that prohibits them from using or giving out information for any reason other than the purpose of the contract.

For example, we may contract with:

1. Print or mail services for customer communications
2. Audit or consulting firms for validating the integrity of our processes
3. We are permitted or required by law to make certain other uses and disclosures of your PHI without your consent or authorization, if we have access, are as follows:
a. For any purpose required by law
b. If required to do so by subpoena or discovery request

How is my Personally Identifiable Information protected?
It is our policy to keep all information about you confidential. It is so important to us that we take the following steps: Our contractors, advisors, trustees, and employees sign an agreement to follow our Rules of Engagement to include strict adherence to confidentiality. We use internal and external auditing (auditors) that reviews our privacy practices. We have information technology security systems in-place to detect and prevent security breaches. All computer systems have security protection configured and installed. All data that you enter on our site is encrypted with the industry-standard encryption technology. By encrypting your data, your data is protected while being transferred over the Internet. We also do not store your information on our servers in a centralized manner.

Non-Personal Data Collected Automatically.
When you access our web sites, we may automatically collect non-personal data (e.g. type of browser and OS used, domain name of the web site from which you came, services most liked by users, requests for new services, number of visits, average time spent on the site, pages viewed). This information is used internally to improve our web sites performance or content.

Your Rights

We maintain no records about your health. Your records are your property. To protect your privacy, Doctor's may check and verify your identity when you have questions or issues about your records.

Right to Inspect and Copy
You have the right to request a copy of the PHI that Doctor's or Provider's keep on your behalf. All requests to inspect or copy must be made in writing and signed by you with proof of government issued form of identification to that Doctor or Provider found in your Team Builder.

Right to Amend
We maintain no records on your PHI to Amend.

Right to Notice of a Breach of Information
We are required to notify you by first class mail or e-mail (if you have told us you prefer to receive information by e-mail), of a breach of your PHI data, if we are made aware. Understand your data is encrypted in your Profile/Wallet and not accessible to us. A breach is any unauthorized acquisition, access, use, or disclosure of information that compromises the security or privacy of your PHI data.

Changes to This Notice
We reserve the right to change the terms of this Notice of Privacy as necessary and to make the new notice effective for all PHI data maintained by us. You may obtain a copy of the current notice from www.careparrot.com, or by mailing a request to the address listed below.

Requests and/or Complaint process
If you have a question, complaint, request to inspect/amend records, or if you believe your privacy rights have been violated, you may contact the CareParrot Privacy Team via email info@careparrot.com.

Cookies
See our Cookie Policy

How to Opt Out of Cookies
If you do not wish to receive cookies, please configure your browser to erase all cookies from your computer's hard drive, block all cookies or to receive a warning before a cookie is stored. If you opt out of cookies, you will still have access to all information and resources on CareParrot and your CareParrot profile.

IP Addresses
We collect and log the IP address of all visitors to our websites. 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 so that we can properly administer our systems and gather aggregate information about how our site is being used, including the pages visitors are viewing. This information is not shared outside of CareParrot. We do not link 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.

Your Consent
By using our website, you are responsible for providing CareParrot with accurate, relevant, quality, and complete personal information. You also, by using our website, consent to the collection and use of the information discussed above by CareParrot. Changes in this policy will be posted on this page so that you may always be aware of what information is being collected, how it is being used, and under what circumstances it is being disclosed.

Third Party Sites
CareParrot may contain links to other web sites. We are not responsible for the privacy practices or the content of other web sites.

Some important laws:
1970 U.S. Fair Credit Reporting Act
1970 U.S. Racketeer Influenced and Corrupt Organization (RICO) Act
1974 Family Educational Rights and Privacy Act (FERPA)
1974 U.S. Privacy Act
1980 Organization for Economic Cooperation and Development (OECD) Guidelines
1984 U.S. Medical Computer Crime Act
1984 U.S. Federal Computer Crime Act (strengthened in 1986 and 1994)
1986 U.S. Computer Fraud and Abuse Act (amended in 1986, 1994, 1996 and 2001)
1986 U.S. Electronic Communications Privacy Act (ECPA)
1987 U.S. Computer Security Act (Repealed by the Federal Information Security Management Act of 2002)
1988 U.S. Video Privacy Protection Act
1991 U.S. Federal Sentencing Guidelines
1992 OECD Guidelines to Serve as a Total Security Framework
1994 Communications Assistance for Law Enforcement Act
1995 Council Directive on Data Protection for the European Union (EU)
1996 U.S. Economic and Protection of Proprietary Information Act
1996 Health Insurance Portability and Accountability Act (HIPAA) (requirement added in December 2000)

1998 U.S. Digital Millennium Copyright Act (DMCA)
1999 U.S. Uniform Computer Information Transactions Act (UCITA)
2000 U.S. Congress Electronic Signatures in Global National Commerce Act ("ESIGN")
2001 U.S. Provide Appropriate Tools Required to Intercept and Obstruct Terrorism (PATRIOT) Act
2002 Homeland Security Act (HSA)
2002 Federal Information Security Management Act of 2002

Several US federal agencies have privacy statutes that cover their collection and use of private information. These include the Census Bureau, the Internal Revenue Service, and the National Center for Education Statistics (under the Education Sciences Reform Act). In addition, the CIPSEA statute protects confidentiality of data collected by federal statistical agencies.