

The Hello Health Electronic Health Record: Security to the Fourth Power

At Hello Health®, we take security seriously. That's why we have developed a comprehensive Four Point security program to protect your clinical data at all levels – from user permissions security and compliance to network and data center security. Here's an overview:

Data Security Your data is hosted at geographically diverse data centers that maintain the highest security standards available, with full disaster recovery, load balancing and real-time back up protocols. Data centers are staffed with onsite guards, and apply biometric and electronic monitoring, and other physical security protocols. Hello Health conducts regular data center reviews by third party auditors to promote conformity with standardized Service Organization Control (SOC) 2 principle criteria. SOC2 replaces the previous SAS 7 standard, and provides a stronger oversight mechanism, so you can rest assured that your data is not vulnerable.

Network Security Hello Health uses the highest-level SSL (Secure Socket Layer) encryption methods to protect you from hackers, malware or other malicious attacks, and encryption is managed at the load-balancer level to improve performance. Real-time audio-video communications and text chats are encrypted using Real-Time Messaging Protocol (RTMP).

User and Access Security Hello Health has designed a role-based access control (RBAC) approach, for restricting system access to authorized users. Access to individual patient information is restricted to the patient, the health care provider or any approved third parties, and data is only accessed through the application layers of our secure servers. Hello Health includes a full auditing process to track every modification to the patient's health record. Session identifiers along with IP addresses are recorded in the database. Unsuccessful login attempts with IP addresses are also recorded, and all data is encrypted based on Meaningful Use standards.

Regulatory Compliance Hello Health fully complies with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and the Meaningful Use security requirements outlined in the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 and validated by the Certification Commission for Health Information Technology (CCHIT®), an Office of the National Coordinator (ONC) authorized certification body. Hello Health employees receive ongoing HIPAA training, and we use third party auditors to regularly review our operations and business processes.



Feel Secure With Hello Health

- 99.9% uptime for our system
- Ongoing third party security assessments
- Meets or exceeds Meaningful Use standards for encryption protocols
 - Full disaster recovery
 - HIPAA compliant

Security in the Cloud: Leave it to Us!

As a web-based solution, Hello Health offers an advantage over our client-server based counterparts. We handle the backups, upgrades, load balancing, and other security protocols from our secure data centers so you don't have to. You eliminate hours and hours each year of Information Technology (IT) headaches, and reduce your overall health information technology investment by eliminating the need for servers and IT staff or consultants. All you need is an Internet connection for secure, on demand access to your clinical data, and our IT professionals will take care of the rest.



Hello Health Inc.
10 Morton Street
New York, NY 10014

hellohealth.com
info@hellohealth.com
877.610.0119

@hellohealth 
facebook.com/hellohealth 

hellohealth®