How hc1 Makes Security and Privacy Our Top Priority

In Every System and Service We Deliver

Introduction

As a HIPAA-regulated company, hc1 Insights, Inc., formerly hc1.com Inc. (hc1) must protect the highly sensitive Protected Health Information (PHI) that our healthcare customers store in our system. Therefore, security must be a priority in every system and service we deliver and in all business processes we follow.

This whitepaper describes hc1's approach to safeguarding customer data. By providing customers with secure, scalable, reliable data access and outstanding performance, hc1's Amazon Web Services (AWS)-based cloud platform allows laboratories, healthcare providers, health systems and other healthcare organizations to focus on improving their business rather than handling security and IT issues.

The approach and information security program described in this whitepaper is extended to the systems hc1 maintains organizations hc1 provides services to and the services these organizations provide to their customers.

To provide further assurance of the manner in which hc1 safeguards customer data, hc1 sought to obtain HITRUST certification for the following platform, location and supporting infrastructure of the hc1 organization:

The hc1 Platform® hosted at Amazon Web Services (AWS) and the hc1 corporate headquarters in Indianapolis, IN

The hc1 Platform hosts all hc1 solutions. Including the solutions hc1 provides to its customer and partners. hc1 Insights, Inc., the hc1 Platform, and the corporate headquarters located in Indianapolis, IN, meet the HITRUST CSF® v9.3 Risk- based, 2-year (r2) certification criteria, receiving a final certification letter effective December 16, 2021. This certification was validated during a third-party, independent interim assessment performed in 2022, receiving a final interim assessment certification letter effective November 19, 2022. The (r2) validated assessment certification is a tailored assessment for the highest level of assurance that an organization may earn from HITRUST.

The assessment performed by a HITRUST Authorized External Assessor and HITRUST's independent confirmation that the work by the external assessor was performed in accordance with the HITRUST® Assurance Program requirements certifies hc1's compliance with the Health Insurance Portability and Accountability Act (HIPAA). The third-party assessment of the hc1 Platform and supporting infrastructure was also validated against an information protection program consistent with the objectives specified in the NIST Cybersecurity Framework v1.1.

HITRUST Overview

The Health Information Trust Alliance Common Security Framework (HITRUST CSF) serves to unify security controls based on aspects of US federal law (such as HIPAA and HITECH), certain state-specific laws, and other industry-standard compliance frameworks into a single comprehensive set of baseline security and privacy controls, built specifically for healthcare needs.

For more information about the HITRUST CSF framework, see HITRUST CSF.

Click this link for a summary of hc1's assessment.

Key Elements of hc1's Approach to Security

The Committee on National Security Systems (CNSS 2010) defines Information Security as "The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification or destruction in order to provide confidentiality, integrity and availability (CIA)." Maintaining the confidentiality of our customers' (and their customers') data and ensuring the integrity and availability of their systems are the primary goals of our security program.

Both the hc1 Platform® and the hc1 organization have the advantage of being built from the ground up for healthcare. This dedication to healthcare means that protecting the integrity of customers' sensitive information has always been an hc1 priority. This pervasive attention to security is driven down from the top of the organization.

Customer Data Confidentiality

hc1 highly values customer data security and treats all customer data as confidential. We do not use any information collected on behalf of a customer except as may be allowed in a contract with that customer.

Integrity and Availability

The ability to secure PHI was built into the hc1 platform from the start, not tacked on as an afterthought. The need to protect this information while maintaining high availability and fast system response informs every architecture and design decision.

Unlike many companies that claim to offer cloud solutions, hc1 is committed to providing a complete platform from one source. For example, hc1 not only monitors what's going on inside of the data center, but also monitors the accessibility of the system from external sources to understand the user experience.

hc1 achieves industry-leading performance by providing:

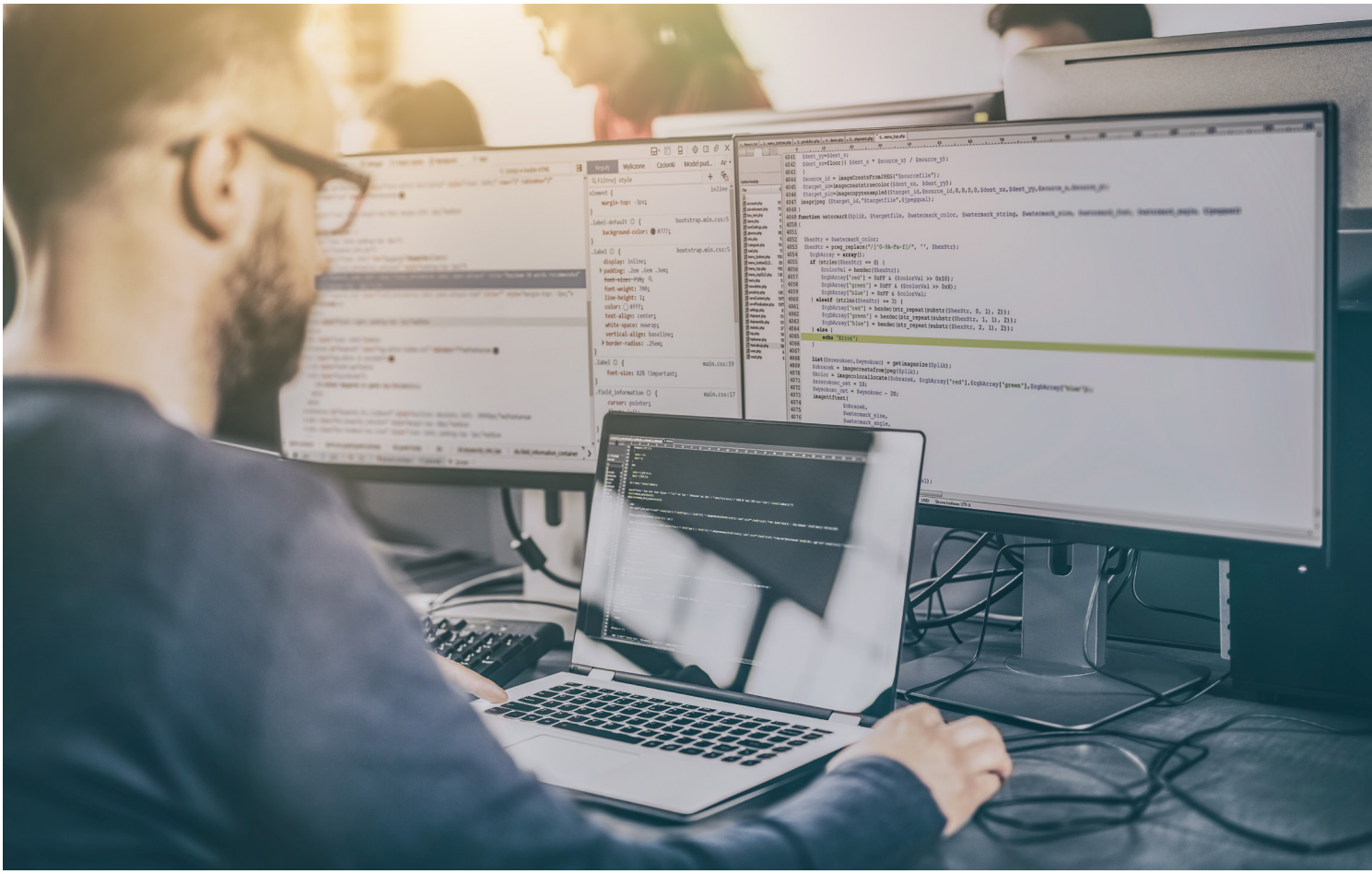
- Contracted service level agreements for uptime and availability
- 24x7x365 real-time internal and external monitoring
- Layered monitoring from the application through the data center
- Redundancy built into all layers of the environment, from the application through the data center
- System and data backups, data restores and disaster recovery

Corporate Security Governance

hc1's corporate security governance is HITRUST certified and aligns with IT, industry and cloud security best practices, ISO27001 the NIST Cybersecurity Framework, in particular.

hc1 System Security

System security is critical because of the data collection, data content serving and reporting activities conducted in the hc1 Platform. In addition, cloud-based delivery often raises concerns for information security. The HITRUST certified hc1 Platform's architecture and design follow industry-standard best practices for security design to address these concerns.



hc1 has been designed for and runs completely in AWS on HIPAA-compliant systems and is covered by our Business Associate Agreement (BAA) with AWS. The hc1 solution leverages all the available security features of AWS and is built to current best practices using a three-tier architecture.

AWS Data Centers

The hc1 Platform is a cloud-based, multitenant, Software as a Service solution that was designed to run exclusively on AWS. AWS operates under a shared security model, wherein it supplies security "of the cloud" while hc1 (and other AWS-based systems) supplies security "in the cloud." In other words, AWS secures the data center and servers where the software is running and makes sure the software is secure for hc1 and its affiliates' customer data.

AWS has more information here: aws.amazon.com/compliance/shared-responsibility-model/

Multiple programs certify AWS data centers. Information about AWS compliance is here: aws.amazon.com/compliance/

Password-Protected Customer Access

Single Sign-On based on either SAML 2.0 or OpenID Connect to a customer's identity provider is preferred. If direct accounts are used, all passwords are encrypted.

Encryption

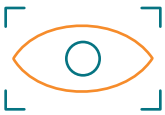
The hc1 Platform provides full encryption of all data in motion and all data at rest, not just data designated as sensitive (such as PHI). All data in transit is encrypted using SSL-TLS version 1.2. To encrypt all data at rest, hc1 employs FIPS 140-2 compliant Amazon EBS encryption.

Log Management

hc1 uses AWS CloudWatch for log management and has implemented a Security Information and Event Management (SIEM) functionality, leveraging Alert Logic's cybersecurity team and solutions. A SIEM concentrates and correlates logging, event notification, and forensic analysis information from critical infrastructure and other security tools.

Firewalls and Load Balancers

hc1 is committed to leveraging as much of the standard AWS infrastructure as possible in the architecture of our system. We use AWS' Security Groups and Elastic Load Balancers for firewall protection. Externally, we leverage a managed Web Application Firewall from Alert Logic.



Service Monitoring

The hc1 Operations Team monitors servers, routers, switches, load balancers and other critical equipment on the network 24x7x365. It also utilizes external services to assure hc1 users can reach the hc1 system. The hc1 Service Level Agreements guarantee that the hc1 system is available for customer use—not simply that the system is "up" or that the infrastructure is functional.

Data Replication and Backup

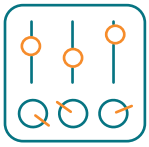
The hc1 platform utilizes near-real-time data replication to ensure hc1 can meet our Recovery Point Commitment in the event of a disaster at our primary AWS data center. hc1 also performs full backups periodically in case a customer's system should ever need to be restored.

Change Management

hc1 uses JIRA to document and track changes in order to increase communication between teams that share resource dependencies and inform relevant parties of pending changes. A Change Approval Board consisting of engineering, technology operations, information security and senior management documents, reviews and approves all changes.

Patch Management

hc1 takes patching seriously, because known vulnerabilities are often the pathway into systems for hackers. hc1 employees monitor both industry-standard notification lists for announced vulnerabilities and associated fixes. We also perform external vulnerability scans and internal credentialed scans at least once a week on hc1 systems. The goal is to patch all systems at least once per calendar month. hc1 generally delivers new software releases to product at about the same frequency and tests hc1 systems throughout the development cycle (test to stage to production). This process also allows hc1 employees to test systems with the patch version of the software prior to go-live. In the event of a zero-day threat, confirming whether hc1 has systems affected and delivering the appropriate patch as soon as possible is the top priority.



Access Controls

Only authorized users with proper credentials and a need to access the systems can access and administer the hc1 infrastructure. Access is requested, approved and tracked via the JIRA ticketing system.

User access is managed based on industry-standard best practices, including requiring strong passwords and 2FA. hc1 conducts periodic user access audits, tracking the de-activation of user accounts via JIRA.

Risk & Vulnerability Management

At the organizational level, hc1 has processes in place to ensure that we manage risk according to healthcare industry standards.

Audits

As a HIPAA-regulated business, hc1 is subject to a rigorous set of requirements designed to ensure the highest level of security for the PHI stored in our systems. In addition, as a HITRUST-certified organization, hc1 and its affiliated companies demonstrate compliance with HIPAA and other industry regulations through rigorous external audits

Penetration Testing

In addition to the frequent automated vulnerability testing we do, hc1 also performs security, vulnerability and penetration testing in conjunction with a third-party vendor to uncover potential security vulnerabilities in hc1 software and systems. Industry best practices are used to complete the tests. Summary results are available upon request.

ALERT LOGIC by HelpSystems

Vulnerability Scanning

hc1 uses the Alert Logic continuous scanning platform to continuously monitor our systems.

Data Loss Prevention

hc1 leverages software, tools and processes to ensure data is not lost, misused or accessed by unauthorized users. For example, hc1 monitors all incoming and outgoing hc1 emails for potentially sensitive data. Likewise, all employees must log on to the corporate VPN when using their laptops to allow for network monitoring.

Incident Response

As per HIPAA regulations, in the event of a security incident, hc1 will take immediate steps to address the situation and will then contact our customer (the Covered Entity) about the event.

Security Policies and Standards

Good policies are important, because they help establish principles that guide decisions and actions across the entire organization. Like most HIPAA-regulated organizations, hc1 has created, published and provided training on a set of Information Security Policies and Information Protection Standards. All of hc1's policies apply to all employees of the company, whether or not they have access to PHI. If department-level policies become necessary, they would be required to align with these corporate policies and be subject to the same oversight.

hc1's policies and procedures are reviewed and approved annually by management and further reviewed by an independent third-party as a part of hc1's annual audit program, including HITRUST's validated assessments.

Training

All of hc1's employees and contractors directly providing services to hc1 or its affiliates (Team Members) are expected to be familiar with HIPAA regulations and, per these regulations, receive regular education and reminders about security best practices. All Team Members go through an annual third-party HIPAA training and certification program and must pass a test on the materials, whether they have access to PHI or not. Security information and updates are published to the team periodically throughout the year and include weekly micro training videos and tests provided by hc1's third-party vendor. Additionally, employees are instructed about how security affects their specific roles within the organization and the company as a whole.

Headquarters Location

The hc1 corporate network is completely separate from the hc1 Platform network. No customer-facing systems are physically located at hc1's office. All of the systems used to run the hc1 business are either cloud-based or operated by service providers. In the event of a disaster at the hc1 office, all employees would be able to provide full service to customers from home.

Access Control and Segregation of Duties

Only authorized hc1 employees can access customer data based on their job function and a "need to know." Control is also enforced by segregation of duties. hc1's Security Team conducts periodic reviews to confirm users with privileged access continue to require that access.

Background Checks

hc1 Human Resources employs a third party to perform full background checks on all candidates for employment. Information is collected and retained about educational background, work history, criminal felony, and misdemeanor history, the results of an SSN trace and validation, the results of a search of global sanctions and national sex offender registries, and the candidate's credit history. These background checks are performed for all Team Members before receiving access to systems.

Conclusion

hc1 proactively protects customer data and provides the best possible security through the use of stringent procedures as described in this paper. The safety of customer data is paramount for the entire company, and our rigorous security processes and tools demonstrate our commitment to protecting this data.