StratoGen

Up Time. On Time. Every Time.

Our Commitment to Information Security

What is HIPPA?

Health Insurance Portability and Accountability Act 1996

The HIPAA Privacy regulations require health care providers and organizations, as well as their business associates, develop and follow procedures that ensure the confidentiality and security of protected health information (PHI) when it is transferred, received, handled, or shared. This applies to all forms of PHI, including paper, oral, and electronic, etc.

The Office of Civil Rights

The Office of Civil Rights (OCR) is charged with enforcing the Health Insurance Portability and Accountability Act (HIPAA). More specifically, OCR enforces the HIPAA Privacy Rule, which protects the privacy of individually identifiable health information; the HIPAA Security Rule, which sets national standards for the security of electronic protected health information; and the HIPAA Breach Notification Rule, which requires covered entities and business associates to provide notification following a breach of unsecured protected health information.

OCR's audit protocol for the Privacy Rule include audit procedures related to notices of privacy practices for protected health information (PHI), rights to request privacy protection for PHI, access to PHI by individuals, administrative requirements, uses and disclosures of PHI, amendment of PHI, and account of disclosures of PHI. For the Security Rule, the requirements for administrative, physical, and technical safeguards are included in the protocol.

The Office for Civil Rights enforces the HIPAA Privacy Rule, which protects the privacy of individually identifiable health information; the HIPAA Security Rule, which sets national standards for the security of electronic protected health information; the HIPAA Breach Notification Rule, which requires covered entities and business associates to provide notification following a breach of unsecured protected health information; and the confidentiality provisions of the Patient Safety Rule, which protect identifiable information being used to analyze patient safety events and improve patient safety.

The HIPAA Compliance report

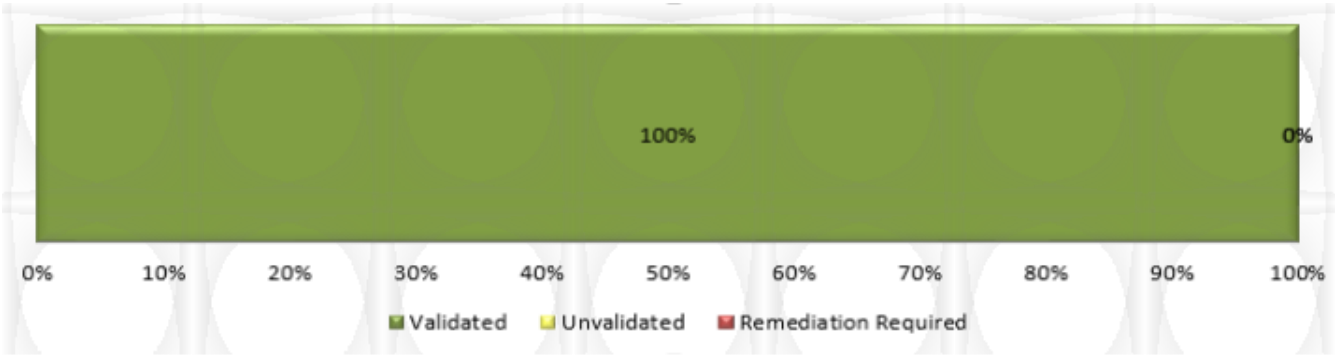
- Identifies an adequate level of security protection for IT applications and systems.
- Meets Federal, State, and U.S. Department of Health and Human Services requirements for information and system security.
- Satisfies oversight organizations.
- Identifies risk and mitigates it to an acceptable level.

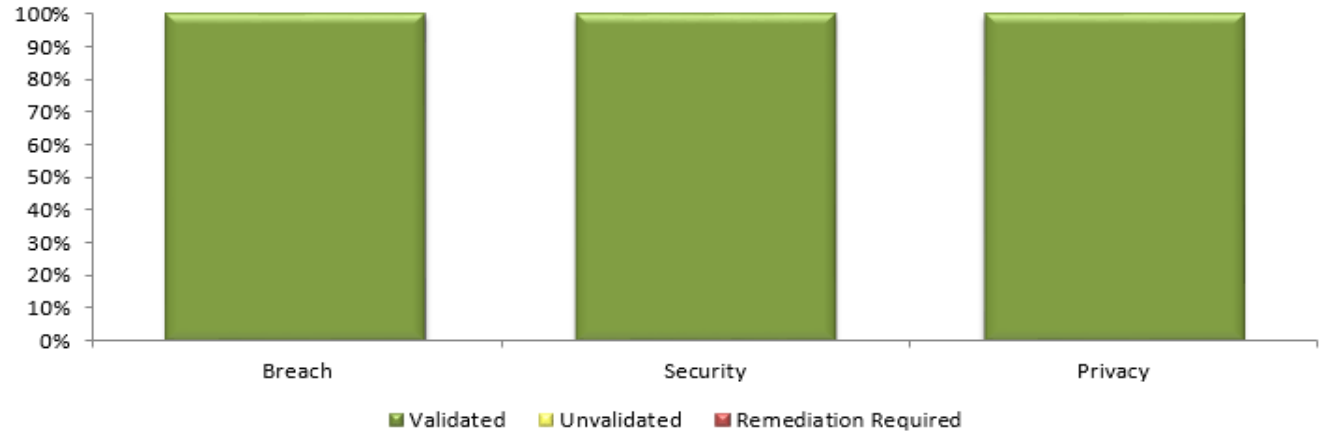
This compliance report is issued after a technical and operational review of Information system vulnerabilities based on a review of legislative requirements, corporate governance, departmental procedures and technical controls. The assessment framework is based on the Health and Human Services audit protocol and covers the HIPAA regulatory text for the Privacy Rule, Security Rule and Breach Notification requirements. The baseline controls utilized for this report were the NIST Security Controls for Federal Information Systems (NIST SP 800-53 rev3).

The HIPAA Report on Compliance focused on the Stratogen Inc. facilities, business process and IT infrastructure for the EHR system. The assessment included a review of the storage, processing or transmitting PHI data within this environment. This review identified data flows, internal business processes and 3rd party connections handled by this information system. Network devices, operating systems and applications involved in supporting these business processes were also included in the scope of this assessment.

The HIPAA Compliance Summary

The graph below represents the current standing of the overall HIPAA compliance status. This graph represents the percentage of HIPAA control items currently in place, including those required during the formal assessment from the Office of the National Coordinator for Health IT (ONC). A more detailed analysis of the specific gaps measured against the HIPAA control items.





What is ISO27001:2013?

It is a specification for an information security management system (ISMS) – a framework of policies and procedures that includes all legal, physical and technical controls involved in an organisations information risk management processes

Customers are increasingly expecting good information security and want to know that any data they share with us is properly protected along with their reputation. This standard that is accepted and trusted in over 160 countries around the world.

Having an Information Security Management System (ISMS) demonstrates a commitment to Information Security that is trusted, transparent and committed and which our clients and prospects can have confidence in.

Annex A of the Standard covers 114 separate controls around the following subjects

1. Risk assessment
2. Security policy
3. Organization of information security
4. Asset management
5. Human resources security
6. Physical and environmental security
7. Communications and operations management
8. Access control
9. Information systems acquisition, development and maintenance
10. Information security incident management
11. Business continuity management
12. Compliance

How do we achieve compliance?

We start at the very top with absolute commitment from our Board and it is Management responsibility to ensure that their own staff are compliant from their very first week

- … Run a robust risk assessment program
- … Conduct internal audits constantly
- … Maintain and communicate our Information Security Policies
- … Include Information Security compliance in Staff Contracts
- … Train those staff during the first week of their employment
- … Ask them to take a test in that week and a refresher annually thereafter
- … Constantly provide training and awareness throughout the business
- … Assess every supplier and business partners own Information Security Controls
- … Are passionate about Data Protection
- … Have security assessed all our offices, buildings and data processing facilities
- … Enforce mobile security
- … Have a strong access control policy that is reinforced by role profiling
- … Have a rigid secure development policy and processes
- … Ensure our network is protected at all times using Firewalls, anti-Malware and AV software
- … Have resilience in our network and supporting functions
- … Don't permit the use of non-encrypted portable media
- … Create a Business Continuity plan for every office
- … Undertake external audits annually
- … Operate an incident register and encourage staff to report incidents no matter how incidental they may seem

For further information or if you have any questions, – please email
Information.Security@theaccessgroup.com