HIPAA Compliance Management

Are you certain about your HIPAA compliance?

ATMP Solutions

ATMP Solutions provides our clients with HIPAA certified and Healthcare Industry recognized talent.

Managing HIPAA compliance is a continuous process. Requirements stem from a number of regulations, standards, best practices, and guidelines. Managing such regulations today requires automated processes that that will help in continuously monitoring for compliance. An automated process which is certain, fast, available, and simple makes managing various compliance requirements easy, leaving business enterprises – large, medium or small, to focus on their core business, competition, and strategies.

What can an automated ATMP Solutions Compliance Management solution do for you?

The software platform provides certain key functions that help the overall process, such as:

✓ Decrease the time to get and stay compliant thus reducing costs associated with the compliance processes; address and adapt to the constantly changing regulatory landscape and achieve compliance with new regulations in significantly less time across business units and geographies

✓ Cloud based "pay–as–you–grow" delivery option - Provides 'Software as a Service' (SaaS) model with on-premises deployment or a completely on-demand cloud based service, requiring very low initial investment with high returns; also ideal for small and medium businesses

✓ Centralized dashboard view of the compliance status drilling down across departments and geographies; generation of reports to demonstrate compliance for regulatory or standard based audits

✓ Provide for Workflow, Document Management, Controls Inventory, Compliance Scanner, and fine-grained access control through a secure Web based interface.

✓ Compliance Scanner scans and integrates compliance related information from various multiple sources and matches them against "Compliance Signatures".

✓ Manage exceptions and activities related to compliance; provide reminders to people for addressing compliance related tasks in an optimal manner

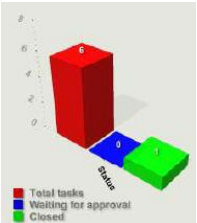✓ Provide an exhaustive audit trail for compliance related actions throughout the whole process

SecureGRC® is a consolidated framework that quickly and cost-effectively enables governance, risk management and compliance (GRC) with one or several government or industry regulations simultaneously.

ATMP *Solutions*

SecureGRC's framework is composed of six tightly integrated components to deliver a highly flexible approach to compliance. The components include:

- *Web-based user interface*
- *Workflow engine*
- *Content and document manager*
- *Access control*
- *Data connectors*
- *Report generator*

Exclusive customer instance of SecureGRC: Each customer on the cloud will have an exclusive instance of the application running ensuring complete security of client data.

Single and centralized repository for all compliance related data: Supports storing all relevant documents, evidences, processes related to compliance in one place with access to it from anywhere and at anytime; organize documents in a hierarchy – whether by geography or department or regulation.

Display questionnaires to evaluate manual controls: Built-in questionnaire generator for use predefined or customized questionnaires. Supports email notifications setup on a schedule to collect information.

Dashboard and reports: Predefined or customized graphs creation facility by the user. The charts have the ability to drill down to the underlying data when clicked and focus on specific departments and geographies.

Reports can also be easily generated and exported to CSV and PDF formats through online interfaces.

Remediation tracking: Tracking issues or "action items" that are either automatically detected or manually found in the compliance management process and remediating through feature-rich remediation module. Items can be assigned to individuals or groups, approved by their managers, fixed, and closed online.

Compliance activity email reminders: Define workflow once in terms of roles and responsibilities and facility to attach documents and provides exhaustive audit trail of actions related to the workflow.

Track Electronic Protected Health Information within databases, file systems, desktops, and servers: Compliance Scanner will search for Electronic Protected Health Information data in file systems, shared drives, databases, and removable hard drives.

External vulnerability scans: SecureGRC® provides for on-demand and scheduled runs of external vulnerability scans for external IP addresses.

Analyze firewall rule sets: Automatically gather information from various supported systems and mapping against the relevant regulations or standards based on one-time setup and scheduling.

Perform vulnerability scans and integrate with existing vulnerability scanners: Gather information from network vulnerability scanners (such as Nessus) and external ASV scans and automatically map them to the relevant regulations.

Integrate with web application scanners: Gather information from web application vulnerability scanners and automatically map them to the relevant regulations.

Compare user access for appropriateness: Compare and check access rights of users and whether they belong to groups that have the appropriate rights for access. Any discrepancies can then be flagged and marked as non-compliant through the use of "Compliance Signatures".

Test password strength of domain and databases: Continuously monitor password strength settings such as alphanumeric requirement, expiry upon 60 days, and account lockout within target databases and operating systems in scope. These settings can be configured to match up with requirements for password strength.

The SecureGRC architecture is designed to deliver highly flexible, enterprise-class performance. It features a multi-threaded architecture, fault tolerance, scalability and an intuitive Web-based interface that non-technical business professionals can use.

Compliance ✓