



STREAMLINING HIPAA COMPLIANCE WITH TRUSTEDAGENT GRC

Achieving and maintaining HIPAA compliance is no longer have to be costly, manual and resource intensive due to the availability of powerful Governance, Risk and Compliance (GRC) solutions. This whitepaper highlights the key capabilities of TrustedAgent GRC to address the HIPAA Security, Privacy and Breach Management requirements enabling healthcare organizations, regardless of sizes, to implement cost-effective HIPAA compliance programs.

Trusted Integration, Inc.
525 Wythe Street
Alexandria, VA 22314
www.trustedintegration.com



Background

Health Insurance Portability and Accountability Act of 1996 (HIPAA) is the federal Health Insurance Portability and Accountability Act of 1996. The primary goal of the law is to make it easier for people to keep health insurance, protect the confidentiality and security of healthcare information and help the healthcare industry control administrative costs. On January 17, 2013, the federal Department of Health and Human Services (HHS) announced a final omnibus rule amending HIPAA in accordance with the HITECH Act of 2009. On March 26, 2013, the HIPAA amendments of 2013 become effective, and added to the existing HIPAA regulations several provisions including HIPAA Privacy, Security, Breach Reporting, and Enforcement Rules. No longer can covered entities and business associates operate outside of compliance to HIPAA/HITECH, as the amendments also establish an enforcement framework for violations of PHI which may extend upward of \$1.5 million a year of any covered entities (CE) or business associates (BA).

HIPAA requires the following entities to comply with the regulations:

- **Health Care Providers:** Any provider of medical or other health Services that bills or is paid for healthcare in the normal course of business. Health care includes preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, services, assessment, or procedure with respect to the physical or mental condition, or functional status of an individual.
- **Health Care Clearinghouse:** Businesses that process or facilitate the processing of health information received from other businesses. It includes groups such as physician and hospital billing services.
- **Health Plans:** Individuals or group plans that provide or pay the cost of medical care and includes both Medicare and Medicaid programs.
- **Business Associates of any Covered Entity** as regulated under the Omnibus Rule.

Meaningful Use (MU) criteria applicable to Electronic Health Records (EHR) also reinforce HIPAA and the safeguards of electronic health information.

The Requirements

HIPAA requirements are organized into different titles or sections that address a unique aspect of health insurance reform. Two main sections are Title I dealing with Portability and Title II that focuses on Administrative Simplification.

Portability allows individuals to carry their health insurance from one job to another so that they do not have a lapse in coverage. It also restricts health plans from requiring pre-existing conditions on individuals who switch from one health plan to another. Administrative Simplification defines a set of standards for receiving, transmitting and maintaining healthcare information and ensuring the privacy and security of individual identifiable information. Most organizations, regardless of size, struggle to meet the specific requirements of outlined in the Administrative Simplification section:

- **Security standards:** Provide administrative, physical, technical and organization safeguards for the protection of electronic protected health information (ePHI).

- Privacy standards: HIPAA provides for the protection of individually identifiable health information that is transmitted or maintained in any form or medium. The privacy rules affect the day-to-day business operations of all organizations that provide medical care and maintain personal health information.
- Breach Reporting: Provides notification requirements in the case of breach of unsecured health information. Breach requirements address individual, media, business associates, and to the federal Secretary of HHS.

The burden of proof for ensuring compliance requires a significant level of effort across the organization. Why? At the highest level organizations are required to have in place effective business processes, management systems, and policies and procedure to conduct risk assessment and risk management, security and incident management, and management and breach reporting. Key business processes and management systems called out under HIPAA include:

- Risk Management Process – Outlines how the organizations identify, assess, mitigate, and monitor risks related to HIPAA.
- Security and Privacy Incident Management – Detect, respond, and report incidents, minimize loss and destruction, mitigate the weaknesses that were exploited, and restore information system functionality and business continuity as soon as possible.
- Management and Breach Reporting – Management reporting is essential to ensuring ongoing compliance. HIPAA expects that senior management involvement as part of the workforce requirements, §168.308(a)(3)(i to ii), as well as its security awareness training, §168.308(a)(5)(i to ii). Furthermore, HIPAA also explicitly specifies that continuous monitoring activities must be incorporated as part of a CAP to ensure effectiveness of risk mitigation.

On a more granular level, organizations must maintain an updated inventory list of software applications and systems (internal and external, as applicable to business associates), and devices where ePHI may reside. The organizations must conduct risk assessment against the items identified in the inventory list to determine the extent of risk associated with the specific HIPAA requirements relating to security and privacy standards. This process represents a comprehensive review of over 200 key HIPAA controls, one example of which is shown below:

§164.312(d) Person or Entity Authentication		
Key Activities	Description	Sample Questions
Determine Authentication Applicability to Current Systems/Applications	<ul style="list-style-type: none"> Identify methods available for authentication. Under the HIPAA Security Rule, authentication is the corroboration that a person is the one claimed. (45 CFR § 164.304). Authentication requires establishing the validity of a transmission source and/or verifying an individual's claim that he or she has been authorized for specific access privileges to information and information systems. 	<ul style="list-style-type: none"> What authentication methods are available? What are the advantages and disadvantages of each method? What will it cost to implement the available methods in our environment? Do we have trained staff who can maintain the system or do we need to consider outsourcing some of the support? Are passwords being used? If so, are they unique by individual?
Evaluate	<ul style="list-style-type: none"> Weigh the relative advantages and disadvantages 	<ul style="list-style-type: none"> What are the strengths and weaknesses of each

§164.312(d) Person or Entity Authentication		
Key Activities	Description	Sample Questions
Authentication Options Available	<p>of commonly used authentication approaches.</p> <ul style="list-style-type: none"> • There are four commonly used authentication approaches available: • Something a person knows, such as a password, • Something a person has or is in possession of, such as a token (smart card, ATM card, etc.), • Some type of biometric identification a person provides, such as a fingerprint, or • A combination of two or more of the above approaches. 	<p>available option?</p> <ul style="list-style-type: none"> • Which can be best supported with assigned resources (budget/staffing)? • What level of authentication is appropriate based on our assessment of risk to the information/systems? • Do we need to acquire outside vendor support to implement the process?

Where risks are identified, organizations must be able to develop corrective action plans (CAPs) for remediation, track the CAP implementation details (i.e., milestones or activities of action, responsible person), and report on progress of CAPs to compliance staff and oversight committees. CAPs must incorporate continuous monitoring to prevent recurrence of incidents. Multiplying the activities outlined above by the number of items in the inventory list, no wonder why so many organizations are drowning in a mix of paperwork and lag in their HIPAA compliance.

HIPAA Workforce by the Number

HIPAA compliance within a hospital system impacts a number of functions including IT Security, Health Information Management, Compliance and Privacy. Trusted Integration conducted a telephone survey of several mid-Atlantic state hospitals to determine the extent in which the hospitals are leveraging HIPAA compliance management software. The hospital systems contacted have beds range from the low 100 to 2,000+ beds. Results indicate that smaller hospital systems (those with beds under 300) are underserved and are still managing HIPAA using manual methods (i.e., spreadsheets, Word documents, etc.).

First, our research survey indicates that, no matter the size of a typical hospital, at least one full time person (FTE) is assigned just to manage HIPAA compliance activities (excluding management). Some hospitals may designate a HIPAA officer for each location, and others may centrally manage the position through the corporate office. Based on the interview, this person has a very high utilization rate due to the manual activities ensuring compliance.

The number of FTEs required to support the HIPAA program tends to increase with increasing number of beds. In our survey, a small range, 125 to 150-bed hospital system, needs between 2 to 3 FTEs (privacy officer, risk manager/compliance officer, and IT security/HIMS person) to support the day-to-day requirements and regulatory reporting of the HIPAA on a part-time basis. From 150 to 300-bed range, we observed similar outcome as seen in 125 to 150-bed range but only with a negligible percentage where the hospital systems utilized HIPAA compliance software for their program.

At the threshold of about 300 beds onward, most hospitals tend to leverage some HIPAA compliance software to lift the burdens of compliance as a means to offset the additional FTEs required to maintain support for the same program. This trend continues to hold with increasing likelihood of existing utilization of software adoption as the number of beds increases above 500 and 1000+ bed ranges. We suspect that the key driver

for adoption in the higher ranges is the greater likelihood for noncompliance due to the combination of complexity of systems, people, and processes.

The survey reveals that smaller hospitals rely on manual process to support existing HIPAA program. The key driver is primarily cost. However, with the prevalence of GRC solutions currently available in the market place, alternatives can be obtained. However, most organizations may be under the perception that a HIPAA software solution is costly and, therefore, choose to maintain status quo.

Security and privacy authorization process requires the organizations to examine their information technology infrastructure and systems, to develop supporting evidence necessary for security and privacy assurance authorization, and a senior official or company management attests to the completion and grants the use of the infrastructure or system. The overall process, while simplistic in definition, can be complex and time-consuming due to the number of activities to be performed. The process also needs resources that strain many organizations by requiring expertise that is both costly and hard to find in today's competitive cybersecurity marketplace. Since the authorization process is continuous in nature requiring ongoing monitoring, update of evidence for changes, and re-testing of controls over time, the organizations incur recurring cost of sustaining the authorization for as long as the IT infrastructure or system is in use.

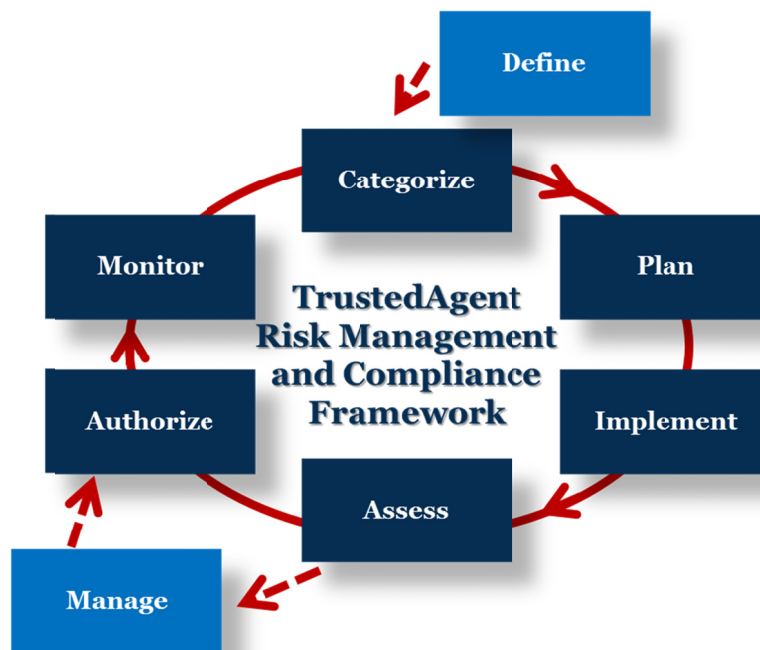
For the public sector, under one or more regulations, including Federal Information Security Management Act (FISMA), Federal Risk and Authorization Management Program (FedRAMP), and Department of Defense Information Assurance Certification and Accreditation Process (DIACAP), Federal government agencies and organizations that provide IT infrastructure and systems to government agencies must meet the requirements of authorization before their infrastructure or systems can be used. In certain cases, where state and local government agencies receiving Federal grants, the agencies must also comply with the requirements of FISMA.

For the private sector, as the governing regulations and standards become more complex and noncompliance penalties range from multiple hundreds of thousands to millions of dollars, many private organizations across several industries including banking institutions, retailers, health care providers, and others are finding themselves under closer scrutiny from their regulators and industry groups to improve their privacy and security practices. Regulations and standards impacting these organizations include Federal Financial Institutions Examination Council (FFIEC), Payment Card Industry Data Security Standard (PCI DSS), North American Electric Reliability Corporation (NERC)'s Critical Infrastructure Protection (CIP), Health Insurance Portability and Accountability Act (HIPAA), and Health Information Technology for Economic and Clinical Health Act (HITECH). For organizations that have already demonstrated ongoing compliance to these standards/regulations, they seek to elevate their standing with their shareholders and industry peers and reduce their liabilities from incidents and data breaches through voluntary adoption of best practices by leveraging one or more frameworks including NIST Cybersecurity Framework (CSF), COBIT, ISO 27001, or SANS Critical Controls.

TrustedAgent as Adaptive, Scalable, Cost-Effective GRC Solution

Since 2001 several major government agencies and commercial companies have relied on TrustedAgent to support their IT security and HIPAA compliance with several regulatory requirements including Federal Information Security Management Act (FISMA), Minimum Acceptable Risk Standards for Exchanges (MARS-E) as published by the Centers for Medicare and Medicaid Services, and HIPAA-HITECH. These clients are major healthcare agencies or players including Centers for Disease Control and Prevention (CDC), Centers for Medicare and Medicaid Services (CMS), National Institutes of Health (NIH), and private companies such as CNSI and Dayna to support CMS Medicare requirements across Washington, Utah, and Maryland states.

TrustedAgent (TA) Risk Management and Compliance Framework (as shown in Figure 1 as dark blue) with the exception of the additional step added for defining the organization inventory and the step for managing findings and their associated corrective actions (as shown in light blue).



Each phase is further described below along with the key HIPAA requirements directly supported.

- 1. Define.** Entities such as information systems, security programs, data centers or vendors are managed within TrustedAgent. Entity characteristics, points of contact, interconnections, hardware and software assets, and architectural/design diagrams are recorded to support the authorization of the entity.

Dashboard

General

Reportable: ☐ Yes ☐ No ☐ All Lifecycle Status: ☒ Operational ☐ Developmental ☐ All Security Category: ☐ Low ☒ Moderate ☐ High ☐ All Include Programs: ☒ Yes ☐ No

Component: South Carolina DHHS Subcomponent: FISMA HIPAA Entity: ISRM Common Controls
ISRM Review System
Magic Kingdom Data Center
Patient Health Management System

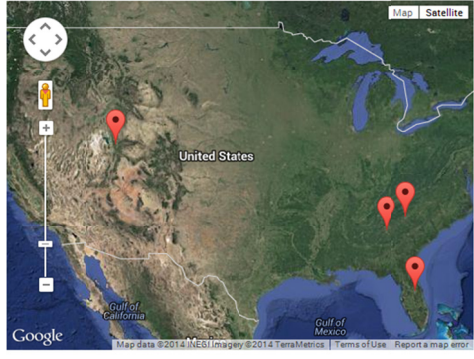
Go **Reset**

Inventory

- Entities
 - South Carolina DHHS
 - All
 - FISMA
 - All
 - ISRM Common Controls (ISRM CC1)
 - ISRM Review System (ISRM Review1)
 - Points of Contact (6)
 - Hardware Assets (4)
 - FXDC-TI-ZCA3 (Hardware)
 - FXDC-TI-ZCA4 (Hardware)
 - FXDC-TI-ZCA1 (Hardware)
 - FXDC-TI-ZCA2 (Hardware)
 - Operating System Assets (4)
 - Software Assets (7)
 - Database Assets (4)
 - Other Assets (1)
 - Subsystems (0)
 - Magic Kingdom Data Center (Disney1)

Create **Edit** **Delete**

Map View

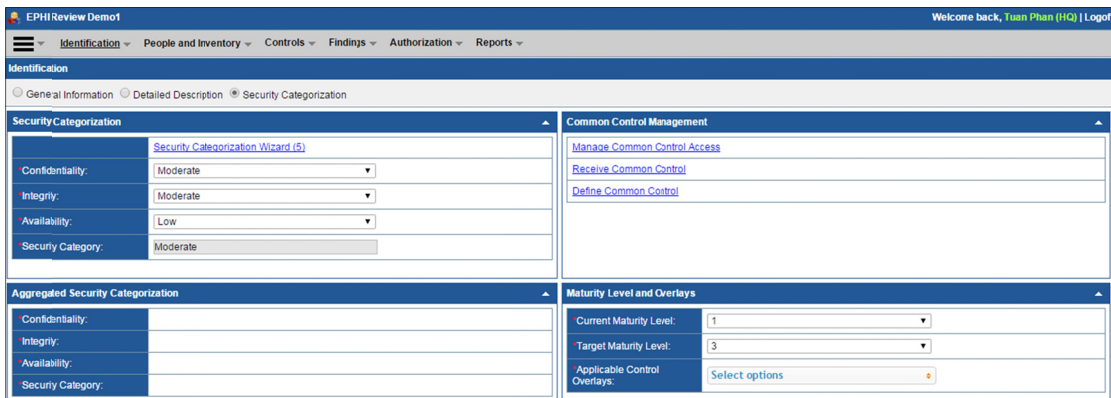


These entities enable the support of the following HIPAA requirements:

Criteria	Key Activity
§164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain and correct security violations	Identify Relevant Information Systems (that house or process ePHI).
§164.308(a)(1)(ii)(B) Security Management Process. Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.306(a).	Implement a Risk Management Program
§164.308(a)(1)(ii)(D) Security Management Process. Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	Develop and Deploy the Information System Activity Review Process
§164.308(a)(1)(ii)(B) Risk Management. Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with Sec 164.206(a).	Acquire IT Systems and Services.
§164.308(a)(6)(i) Security Incident Procedures. Implement policies and procedures to address security incidents.	Determine Goals of Incident Response. Develop and Deploy an Incident Response Team or Other Reasonable and Appropriate Response Mechanism.
§164.312(b) Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	Determine the Activities that Will be Tracked or Audited. Select the Tools that Will be Deployed for Auditing and System Activity Reviews. Develop and Deploy the Information System Activity Review/Audit Policy.
§164.402 - Definitions - Breach means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which	Risk Assessment of Breach

Criteria	Key Activity
compromises the security or privacy of the protected health information. (1)(i) For purposes of this definition, compromises the security or privacy of the protected health information means poses a significant risk of financial, reputational, or other harm to the individual. (ii) A use or disclosure of protected health information that does not include the identifiers listed at §164.514(e)(2), date of birth, and zip code does not compromise the security or privacy of the protected health information.	

- 2. Categorize.** Security categorization processes are employed to determine applicable security requirements. TrustedAgent automates categorization processes using NIST 800-60 or optionally organizations may employ maturity models, thereby significantly reduces the time and error typically associated with these complex processes.



The screenshot displays the 'EPHI Review Demo1' application interface. The top navigation bar includes tabs for Identification, People and Inventory, Controls, Findings, Authorization, and Reports. The 'Identification' tab is selected, and the 'Security Categorization Wizard (5)' is the active sub-tab. The wizard is divided into two main sections: 'Security Categorization' and 'Common Control Management'. The 'Security Categorization' section contains fields for Confidentiality (Moderate), Integrity (Moderate), Availability (Low), and Security Category (Moderate). The 'Common Control Management' section includes links for 'Manage Common Control Access', 'Receive Common Control', and 'Define Common Control'. Below these sections, there is an 'Aggregated Security Categorization' section and a 'Maturity Level and Overlays' section. The 'Maturity Level and Overlays' section includes dropdowns for 'Current Maturity Level' (set to 1) and 'Target Maturity Level' (set to 3), along with a 'Select options' button for 'Applicable Control Overlays'.

Controls are defined based on predefined organizational templates that can be tailored across the various components and business units within the organization. Categorization supports the following requirements:

Criteria	Key Activity
§164.308(a)(1)(i) Security Management Process. Implement policies and procedures to prevent, detect, contain and correct security violations	Identify Relevant Information Systems (that house or process ePHI). Have the types of information and uses of that information been identified and the sensitivity of each type of information been evaluated? (See FIPS 199 and SP 800-60 for more on categorization of sensitivity levels.)
§164.308(a)(8) Evaluation. Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that established the extent to which an entity's security policies and procedures meet the requirements of this subpart	Determine Whether Internal or External Evaluation Is Most Appropriate. Develop Standards and Measurements for Reviewing All Standards and Implementation Specifications of the Security Rule.

- 3. Plan.** Controls are assigned to support staff. Common controls are defined for the enterprise and used by various entities. Controls are tailored as needed for the entity.

Criteria	Key Activity
§164.308(a)(8) Evaluation. Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information...	Develop Standards and Measurements for Reviewing All Standards and Implementation Specifications of the Security Rule.

- 4. Implement.** The controls are implemented and documented accordance with organizational and regulatory requirements. System security plans or other organizational documents can be generated to report on control implementation status and compliance details. The following HIPAA requirements are supported:

Criteria	Key Activity
§164.308(a)(8) Evaluation. Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that established the extent to which an entity's security policies and procedures meet the requirements of this subpart.	Conduct Evaluation.
§164.312(b) Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	Implement the Audit/System Activity Review Process.
Meaningful Use Core Objective & Measure #15: Protect electronic health information created or maintained by the certified EHR technology through the implementation of appropriate technical capabilities.	Conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1) and implement security updates as necessary and correct identified security deficiencies as part of its risk management process.

- 5. Assess.** Controls are assessed by independent assessors. Control Assessment Plan, Security Assessment Results (SAR), and other organizational documents can be utilized and tailored by system owners for their information systems. Findings are recorded and discussed with system owners. Findings that are accepted and converted to corrective actions where they are tracked for remediation purposes. HIPAA requirements supported here are similar to those discussed in Step 4.
- 6. Manage.** Incidents or issues identified by internal (security incidents) or external parties (such as customer complaints) can also be tracked and managed as findings. Findings are either accepted or rejected by system owners. Corrective actions (CAPs), or remediation plans, are generated for accepted findings. CAPs are created for controls that are not Fully Satisfied and where risks have not been accepted by the authorizing official, or have legal or regulatory consequences if not addressed.

Executive Summary or other organizational documents including privacy documents can be created from predefined templates to document the recommendation for the authorization of the entity.

Criteria	Key Activity
§164.308(a)(1)(ii)(A) Risk Analysis. Conduct an accurate and thorough assessment of the potential risks and vulnerabilities	Conduct Risk Assessment

Criteria	Key Activity
to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.	
§164.308(a)(1)(ii)(B) Security Management Process. Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).	Implement a Risk Management Program
§164.308(a)(6)(ii) Security Incident Procedures. Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes.	Develop and Implement Procedures to Respond to and Report Security Incidents. Incorporate Post-Incident Analysis into Updates and Revisions.
§164.402 - Definitions - Breach means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information. (1)(i) For purposes of this definition, compromises the security or privacy of the protected health information means poses a significant risk of financial, reputational, or other harm to the individual. (ii) A use or disclosure of protected health information that does not include the identifiers listed at §164.514(e)(2), date of birth, and zip code does not compromise the security or privacy of the protected health information.	Risk Assessment of Breach
§164.530(d)(1) Standard for Complaints to the Covered Entity. A covered entity must provide a process for individuals to make complaints concerning the covered entity's policies and procedures required by this subpart and subpart D of this part or its compliance with such policies and procedures or the requirements of this subpart or subpart D of this part.	Complaints to the Covered Entity
§164.530(e)(1) A covered entity must have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity or the requirements of this subpart.	Have a process by which individuals can make complaints about its P&Ps or its compliance with P&Ps.
164.530(f) Mitigation. A covered entity must mitigate, to the extent practicable, any harmful effect that is known to the covered entity of a use or disclosure of protected health information in violation of its policies and procedures or the requirements of this subpart by the covered entity or its business associate	Mitigate known harmful effects from violations of its P&Ps and the Privacy Rule by its workforce and business associates.

- 7. Authorize.** The authorization package is presented to the authorizing official for review and approval. Approval letters and waivers are created from predefined templates that document the accreditation decision for the entity along with residual risks that was accepted and granted. Assessment and authorization security metrics (i.e., statuses, dates, and approvals) are recorded for the entity. Key artifacts supporting compliance can be tracked and served as body of evidence of compliance.

Criteria	Key Activity
§164.404 to §164.410 Notification to Individuals, Media, Secretary of HHS and Business Associates.	Develop Standards and Reporting templates to ensure proper and timely reporting meeting the breach notification requirements.

§164.414 Administrative requirements and Burden of Proof. In the event of a use or disclosure in violation of subpart E, the covered entity or business associate, as applicable, shall have the burden of demonstrating that all notifications were made as required by this subpart or that the use or disclosures did not constitute a breach as defined at §164.402.

Burden of Proof

- 8. Monitor.** Ongoing security reviews, assessments, and remediation of vulnerabilities and corrective actions are performed. Results of vulnerability assessments, independent audits, and continuous monitoring assessments are managed with risk management oversight performed by the organization. Corrective actions are remediated and updated by system owners.

Criteria	Key Activity
§164.308(a)(8) Evaluation. Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that established the extent to which an entity's security policies and procedures meet the requirements of this subpart	Conduct Evaluation.
§164.312(b) Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	Implement the Audit/System Activity Review Process.
§164.530(i)(2) Changes to Policies and Procedures. §164.530(i)(3) Changes in Law §164.530(i)(4) Changes to Privacy Practices §164.530(i)(5) Changes to Other Policies or Procedures	Manage changes related to P&P, Laws, Privacy Practices and Others.

TrustedAgent also supports the specification of key and standard controls required to be assessed for a given assessment period (calendar or fiscal year). Dashboard and other reporting features are available for users to filter controls required to be assessed based on their assigned continuous monitoring period and type. Control continuous monitoring efforts can be setup in TrustedAgent across a three year cycle. Below is an example for how control continuous monitoring can be established within TrustedAgent.

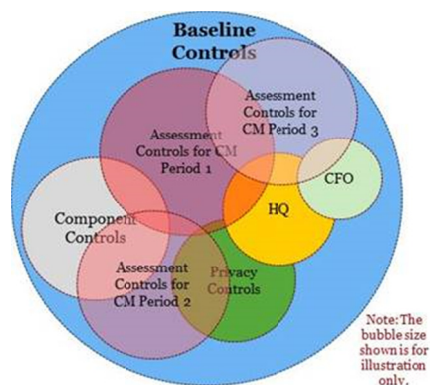


Figure 1: Control Continuous Monitoring Composition

TrustedAgent also supports vulnerability assessment imports in the form of the scanner's native XML output file. The following vulnerability assessment scanners are currently supported:

- Nessus
- Saint
- OpenVAS
- eEye Retina
- AppScan
- Rapid7
- AppDetective

Support for other scanners can be added through the addition of a XML connector (configuration mapping file).

Additional Key Benefits with TrustedAgent

Regulatory Document and Report Generation

TrustedAgent is capable of generating regulatory compliance documents and reports based on initial templates provided by Trusted Integration and/or based on templates created by power users of the application. Specifically to the organization's requirements, TrustedAgent provides and supports the automation of HIPAA/HITECH regulatory compliance templates (with all applicable controls) including:

- System security plans (with hardware and software asset lists)
- Security assessment report (with associated findings and risk exposure rating)
- Contingency plan
- Requirement traceability matrix
- Privacy documents
- Rules of Behavior

By leveraging the Content Framework below, any number of regulatory documents and management reports can be developed to meet the specific requirements of the organization.

TrustedAgent Content Framework

The TrustedAgent content framework, pictured below, contains information supporting a full lifecycle of any risk and compliance management process. TrustedAgent content framework comprises of two major components: TrustedAgent Control Content and TrustedAgent Authorization Content.

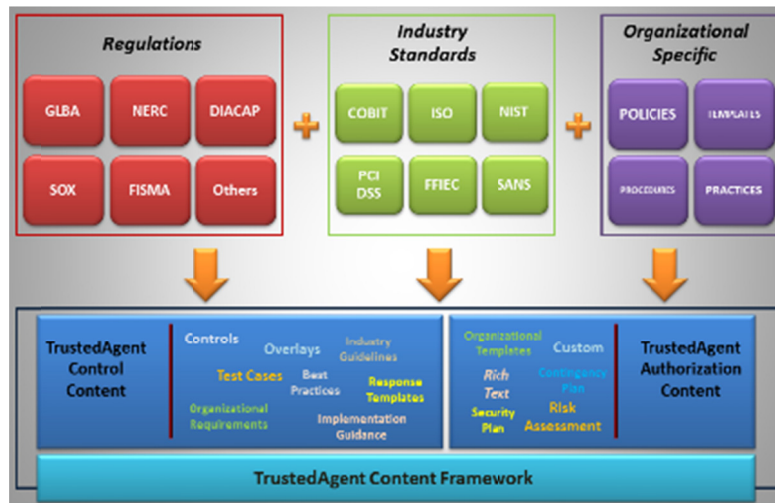


Figure 2: Content Management Framework

The control content, shown above, manages data associated with the controls to the TrustedAgent Platform, and delivers this content along with user information and the authorization content, as shown below, as templates for reporting.

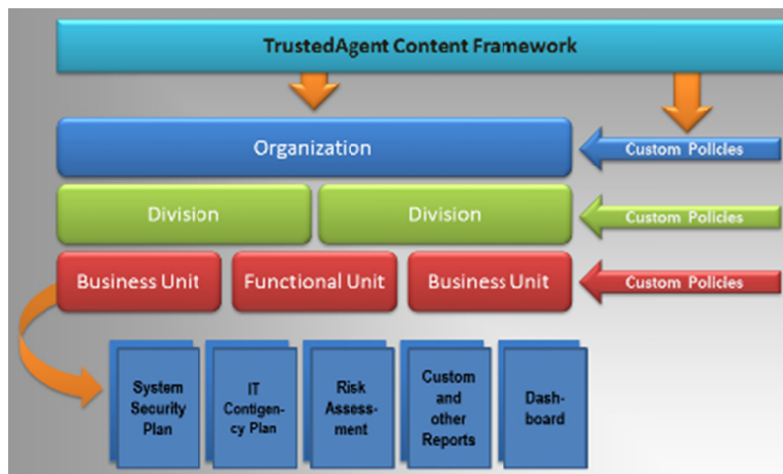


Figure 3: Content Template Deployment

Policy and Procedure Management

Users with content permission can author new policies/procedures or revise existing policies/procedures, customizable to organization's requirements, for their assigned organization, or division/business unit. This capability enables the organization to benefit from having a centrally managed repository of customized policies and procedures as well as security authorization, and control templates.

Template Content

- Document Detail
- Support Documents
- Header / Footer

POL_009

Title

Information Access Management

Version

1

Type

Policy

Originating Component

South Carolina DHHS

[Copy](#)

[Delete](#)

**TRUSTED
INTEGRATION**

INFORMATION ACCESS MANAGEMENT

Effective Date	Version	Description	Author
mm dd/yyyy	1.0	Document Published	Program Office

I. POLICY STATEMENT

It is the policy of the organization to maintain information access controls creating the ability to know whom and when a person may view, modify, or disclose that information.

Figure 4: Policy and Procedure Authoring

Management Dashboard and Reporting

TrustedAgent offers a comprehensive management reporting framework that includes filter-enable drill-down graphical dashboard of key metrics in real-time and historical trends, a plethora of built-in reports, and on-demand (ad hoc) reports using organization-defined criteria/queries.

TrustedAgent's dashboard organizes key metrics into views relating to Authorization, Inventory, Assets, Controls, Findings, and Corrective Actions. These views are provided with filters and drillable details allowing visualization of information in an easy to understand manner.



Figure 28- Sample Regulatory Compliance Dashboard

Workflows and Notifications

Maintain situational awareness is essential in ensuring ongoing compliance with HIPAA requirements. TrustedAgent offers event-based notifications to assist users to manage activities related to a typical security authorization process, and enable the users to prioritize and stay ahead of activity completion due dates. Notifications address all key workflows including information and interconnection, points of contact, assets, controls, findings, corrective actions, milestones and authorization. Notifications also extend to key data summaries allowing audit or oversight staff to track activity progress across the organization.

Notifications are configurable, enabling users to receive more or less notifications, or only specific notifications, or notifications based on selected fields and statuses to best match the user role assigned role within the organization.



<input checked="" type="checkbox"/> Corrective Action Alert	<input checked="" type="checkbox"/> Milestone Alert
<input checked="" type="checkbox"/> Controls Alert	<input checked="" type="checkbox"/> Authorization Alert
<input checked="" type="checkbox"/> POC Alert	<input checked="" type="checkbox"/> User Access Alert
<input checked="" type="checkbox"/> Entity Information Alert	<input checked="" type="checkbox"/> Finding Alert
<input checked="" type="checkbox"/> Interconnection Alert	<input checked="" type="checkbox"/> Asset Inventory Alert
<input checked="" type="checkbox"/> Activity Summary Alert	<input checked="" type="checkbox"/> Change Summary Alert
<input checked="" type="checkbox"/> Quality Alert	

Figure 5: Notification Management

Conclusion

By leveraging the right HIPAA compliance management solution, HIPAA activities can be streamlined significantly in terms of time and errors while delivering cost and resource efficiency. The IT investment does not have to be significant due to the changing competitive landscape. Unlike major players, where the cost of a fully deployed solution may require several hundreds of thousands dollars and several months of planning and follow-up deployments, affordable and equally capable solutions can be sourced from the smaller players, such as Trusted Integration.

The highly scalable and customizable TrustedAgent provides the optimal solution for any organization seeking a balance of between cost, expected requirements, and implementation time to support the HIPAA compliance program:

- Integration of key compliance processes under one centralized risk management framework, allowing the organization to manage compliance and risk activities under one comprehensive, standardized, and enterprise-wide approach.
- Optimize workforce supporting compliance activities by eliminating information silos and duplications of compliance activities.
- Gain visibility and timely access to information to support clear, data-oriented risk-based decisions.
- Demonstrate tangible and rigorous management of governance, risk and compliance activities to senior management, board of directors, and regulators.
- Reduce likelihood of penalties from regulatory bodies.

Trusted Integration is a boutique provider of Governance, Risk and Compliance (GRC) management solutions for highly-regulated government and commercial organizations. Our flagship product, TrustedAgent GRC, is an adaptive, scalable GRC solution for organizations to standardize business processes, reduce complexities, and lower costs in the management, analysis, and remediation of risks across the enterprise.

TrustedAgent provides an unparalleled and cost-effective enterprise solution that enables organizations to inventory, assess, remediate, and manage risks and regulatory requirements before detrimental loss are sustained by the organization.



Trusted Integration, Inc.
525 Wythe Street
Alexandria, VA 22314
703-299-9171 Main
703-299-9172 Fax
www.trustedintegration.com