HIPAA and Its Impact on IT Organizations

How Identity and Access Management Systems Can Play an Important Role in the HIPAA Compliance

Netegrity Technical White Paper
December 18, 2003
# Table of Contents

- HIPAA Background.......................................................................................................... 3
- HIPAA Security and Privacy Overview ............................................................................. 4
- Understanding the HIPAA Final Security Rule............................................................... 4
- Understanding HIPAA Final Privacy Rule....................................................................... 7
- How Netegrity's IAM Solution Meets the Security and Privacy Requirements of HIPAA .... 7
- HIPAA Timelines and Approach.................................................................................... 8
- Conclusion ..................................................................................................................... 9
- Appendix..................................................................................................................... 10
HIPAA Background

The Health Information Portability and Accountability Act of 1996 (HIPAA) had specific goals to improve elements of the healthcare system in the U.S. that included:

- Guaranteed health insurance coverage of company employees;
- Reduced levels of fraud, waste, and abuse in the healthcare industry;
- Administrative simplification across the healthcare industry to improve its efficiency and effectiveness; and
- Protection of the health related information of individuals (i.e., Protected Health Information, or PHI) against access without consent and authorization.

While HIPAA was enacted in 1996, only recently have the final rules for the security and privacy portions of it been published by the Department of Health and Human Services (DHHS).

HIPAA requires “covered entities” (e.g., health plans (including self-insured companies), healthcare clearinghouses, and healthcare providers) that electronically maintain or transmit PHI to ensure the integrity and confidentiality of this information. As a result a large number of organizations in the United States are affected by HIPAA.

Specifically, HIPAA specifies a control environment in which organizations must manage their relationships with internal and external users throughout their lifecycle with the company, from identity creation to access termination. Given that much of PHI is handled electronically with most organizations, how this digital information and the related identities are managed and accessed, becomes a key component of overall HIPAA compliance. This white paper will focus on how Identity and Access Management (IAM) solutions in general and Netegrity’s IAM solution set in particular can assist covered entities with HIPAA compliance.

IAM solutions, such as those from Netegrity, help to secure access to enterprise information assets and help to manage the digital identities of users accessing those assets. IAM systems bring together people, processes, and technologies to enable the control environment required by HIPAA. Consistent with the requirements of HIPAA, IAM solutions generally provide: user management and provisioning, password and entitlement management, authorization management, authentication management, and auditing and reporting services. As a result of these capabilities, IAM solutions are highly relevant to HIPAA compliance efforts.

While there are significant cost-saving and other benefits from implementing IAM solutions, the need to comply with laws and regulations, such as HIPAA, may be the most compelling business driver for IAM in the near term.

As with all laws and regulations each organization must determine whether a specific law or regulation applies to it, and if so, must interpret for itself the specific requirements set forth in the regulation. Therefore, every organization is encouraged to conduct the proper legal analysis with the aid of legal counsel to determine the appropriate application of the HIPAA security and privacy rules to its organization.

This paper presents a detailed overview of the final HIPAA security and privacy regulations and also provides an analysis of how Netegrity’s IAM solutions can help covered entities address these requirements.

Because of the changes between the proposed security and privacy regulations for HIPAA and the final regulations, it should be noted that this paper supercedes a previous publication by Netegrity, entitled, *Obtaining Compliance for HIPAA Technical Security Services*, dated June 2001.
HIPAA Security and Privacy Overview

DHHS published proposed regulations – a security version in 1998 and a privacy version in 1999, which were finalized in 2003. While the IAM related requirements for HIPAA are mostly set forth in the final security rule published on February 20, 2003 (the “Final Security Rule”), elements of the final privacy rule published on August 14, 2002 (the “Final Privacy Rule”) also have IAM implications. As noted in the Final Security Rule, “security and privacy are inextricably linked.” Whereas the security standards focus on the administrative, physical, and technical safeguards to protect electronic PHI, the privacy standards focus on uses and disclosures of all forms of PHI, not just electronic PHI.

More importantly, despite the different compliance dates initially for each rule, it is generally recommended that compliance be evaluated against 45 CFR Part 164 - Security and Privacy in its entirety. This approach will enable a more comprehensive IAM strategy. As noted in the Final Security Rule, DHHS has made, “substantial efforts to ensure that the many requirements in the security standards parallel those for privacy, and can easily be satisfied using the solutions for privacy.”

Understanding the breadth of organizations impacted by HIPAA is also important. Healthcare providers (e.g., hospitals, group practices), payer organizations (e.g., insurance carriers, Blue Cross Blue Shield companies, HMOs) and claims clearinghouses are considered “covered entities” by HIPAA. Other organizations not included in the above list may not necessarily see themselves as part of the healthcare industry and may assume incorrectly that they are not required to comply with HIPAA.

However, companies that manage their own healthcare insurance and/or are self-insured (e.g., plan sponsors) may be impacted by the HIPAA security and privacy regulations if they have access to employee health information. Likewise, the HIPAA security and privacy regulations are clear that third parties (e.g., agents, subcontractors) with access to electronic PHI must also comply with the requirements.

Understanding the HIPAA Final Security Rule

The Final Security Rule contains both “standards” and “implementation specifications”. A HIPAA standard is meant to be comprehensive and scalable and to apply to all covered entities. Implementation specifications provide instructions on how the standards are to be implemented. In some cases the standard is straightforward enough not to require an implementation specification. However, those implementation specifications noted as “Required” must be implemented as written.

Other implementation specifications considered as “addressable” have some flexibility on how that standard should be implemented. The “how” is dependent upon a thorough security risk assessment for the particular organization. In these areas, the covered entity must determine whether the implementation specification is “a reasonable and appropriate security measure to apply within its particular security framework.”

For the most part, the Final Security Rule does not specify the types of security measures to be employed (e.g., type of authentication mechanism, type of authorization approach). Rather, DHHS has required covered entities to conduct security risk assessments and deploy those systems and processes that are appropriate for the particular organization.

As an example, it is expected that a covered entity would apply the appropriate authorization approach based on its risk assessment. Any IAM solution considered as a portion of a HIPAA compliance program should have the authorization and authentication capabilities to support the flexibility and evolutionary approach that is envisioned by the Final Security Rule.
In the final regulation DHHS has confirmed that a covered entity must address access from remote locations. With the increased use of the Internet for remote information access, Internet focused IAM systems and related processes must be considered in connection with HIPAA compliance.

Not only would this requirement affect remote employees who have access to PHI because of their job function (e.g., doctors, claims adjusters, benefit administrators), but it would also affect employees of plan sponsors who are given access to their own PHI remotely through the public Internet or through a private extranet or intranet.

With the Final Security Rule, 45 CFR Part 164 now includes a new Subpart C, which in turn includes a number of sections that apply directly to IAM systems and processes. The sections, asterisked (*) in the list below, have IAM implications that are outlined in detail throughout the remainder of this paper.

- 164.302 – Applicability
- 164.304 – Definitions *
- 164.306 – Security standards: General rules *
- 164.308 – Administrative safeguards
  - Security management process
    - Risk analysis
    - Risk management
    - Sanction policy
    - Information system activity review *
  - Assigned security responsibility
  - Workforce security
    - Authorization and/or supervision *
    - Workforce clearance procedure *
    - Termination procedures *
  - Information access management
    - Isolating healthcare clearinghouse functions *
    - Access authorization *
    - Access establishment and modification *
  - Security awareness and training
    - Security reminders
    - Protection from malicious software
    - Log-in monitoring *
    - Password management *
  - Security incident procedures
    - Response and reporting *
  - Contingency plan
    - Data backup plan
    - Disaster recovery plan
    - Emergency mode operation plan
    - Testing and revision procedures
    - Applications and data criticality analysis
  - Evaluation
  - Business associate contracts and other arrangements
    - Written contract or other arrangement
- 164.310 – Physical safeguards
  - Facility access controls
    - Contingency operations
    - Facility security plan
    - Access control and validation procedures
    - Maintenance records
Workstation use
Workstation security
Device and media controls
  • Disposal
  • Media re-use
  • Accountability
  • Data backup and storage

164.312 – Technical safeguards
  • Access control
    • Unique user identification *
    • Emergency access procedure *
    • Automatic logoff *
    • Encryption and decryption
  • Audit controls *
  • Integrity
    • Mechanism to authenticate electronic PHI
  • Person or entity authentication *
  • Transmission security
    • Integrity controls
    • Encryption

164.314 – Organizational requirements
164.316 – Policies and procedures and documentation requirements
164.318 – Compliance dates for the initial implementation of the security standards*

*Has IAM implications for a typical organization

IAM teams seeking to comply with HIPAA security and privacy regulations should be cognizant of the specific definitions in 164.304 that are applied to terms such as Access, Administrative Safeguards, Authentication, Confidentiality, Password, Technical safeguards, and User. These definitions are provided below:

• **Access** – the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource.
• **Administrative safeguards** – administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic PHI and to manage the conduct of the covered entity's workforce in relation to the protection of that information.
• **Authentication** – the corroboration that a person is the one claimed.
• **Confidentiality** – the property that data or information is not made available or disclosed to unauthorized persons or processes.
• **Password** – confidential authentication composed of a string of characters.
• **Technical safeguards** – the technology, and the policies and procedures for its use that protect electronic PHI and control access to it.
• **User** – a person or entity with authorized access.

The final regulations do provide for a flexible approach on how the security standards in general (164.306) are to be implemented. The security standards whenever possible consider factors such as: size, complexity, and capabilities of the covered entity; the covered entity's technical infrastructure, hardware, and software security capabilities; the costs of security measures; and the probability and criticality of potential risks to electronic PHI.
This paper includes a table, found in the Appendix, with a specific set of requirements from the administrative safeguards (164.308) and technical safeguards (164.312) sections of the Final Security Rule that relate to IAM and how Netegrity’s solutions can help an organization address these requirements.

**Understanding HIPAA Final Privacy Rule**

The privacy regulations are also part of 45 CFR Part 164 (Subpart E). Most of Subpart E discusses the use and disclosure of PHI in specific situations and cases. There are some general requirements of the Final Privacy Rule, as discussed below, that can best be met with the assistance of IAM solutions.

Section 164.514 outlines the minimum necessary requirements, and provides that a covered entity must be able to identify those individuals in the workforce who need access to health data and “must make reasonable efforts to limit access of such persons”. An IAM solution that allows access to be managed by job role or according to a specific business rule could address this need.

This section also outlines the need for identity verification of any individual requesting PHI disclosures, particularly if the individual is not known by the covered entity. An IAM solution with the ability to support access through a flexible authentication and authorization model, including the support of federated security, could address this need.

Another general requirement related to privacy is the need by the covered entity to provide individuals with access to their own PHI (164.524). Not only do individuals have a right to their data, but also they can expect access to that information quickly, efficiently, and in a manner that is secure. Web access through the Internet is certainly one way to meet this requirement. An IAM solution can cost effectively provide covered entities the secure access capability to help meet this need.

Finally, the privacy administrative requirements (164.530) include a general safeguard standard that requires a covered entity to reasonably safeguard PHI from any intentional or unintentional use or disclosure. The functionality contained in an IAM solution can also help to address this general privacy requirement.

Advanced authorization management techniques (e.g., roles, rules/policies) may provide the fine-grained control that the general privacy safeguards, noted above, require of covered entities. These techniques will be necessary for covered entities to be effective in providing approved people only the minimum access necessary to complete their job tasks.

**How Netegrity’s IAM Solution Meets the Security and Privacy Requirements of HIPAA**

IAM solutions, such as those available from Netegrity, should be evaluated against the specific requirements outlined in the final security and privacy regulations if they are being considered as a tool for HIPAA compliance.

The value of Netegrity’s solution for assisting with HIPAA compliance is best understood by mapping the functionality of its IAM solution to the relevant requirements found in the final HIPAA security and privacy regulations (45 CFR Part 164). Tables 1 and 2 found in the Appendix at the end of this white paper provide specific IAM standards and implementation specifications from both the Final Privacy Rule and the Final Security Rule, and describe how Netegrity’s IAM solution can help an organization meet these requirements.
It should be noted that some of the language contained in the two tables regarding the regulations has been modified (e.g., dropping references to other sections or other laws, simplifying the legal language) but not changed in a way that alters the intent of the regulation. However, readers are advised to consult the specific language of each regulation.

Netegrity provides an integrated IAM solution that is comprehensive in scope for legacy, Web, and service-oriented architectures. With a strong commitment to standards, Netegrity provides components for access management, Web services security, user administration, and resource provisioning in an integrated solution.

Netegrity’s IAM components include:

**SiteMinder** - SiteMinder's advanced security policy and management capabilities, proven reliability and scalability, and broad technology and standards support, enables rapid development, deployment, and management of sophisticated Web security software systems, enabling the delivery of essential information and applications to employees, partners, customers, and other users across the enterprise.

**TransactionMinder** - Similar to SiteMinder in architecture, TransactionMinder software provides a secure and centralized, policy-based authentication and authorization management capability for Web services. TransactionMinder integrates with standard Web services frameworks and provides fine-grained access control for XML documents across multi-step business transactions.

**IdentityMinder** - IdentityMinder's advanced user management capabilities enable the rapid development, deployment, and management of a sophisticated user and entitlement management software systems, enabling the efficient and secure delivery of essential Web applications, enterprise resources and information, and physical assets to users.

**HIPAA Timelines and Approach**

While the security and privacy regulations do consider certain criteria (e.g., the size of the health plan) that may impact the compliance deadline, compliance with the Final Security Rule is generally required by April 21, 2005 and compliance with the Final Privacy Rule was generally required by April 14, 2003.

For those concerned with IAM systems and processes, this means that compliance with 45 CFR Part 164 - the implementation of security and privacy requirements as an integrated set of requirements - should do so as fast as possible so as to avoid separate, redundant or piecemeal efforts to comply with the two sets of regulations.

Some covered entities may feel a bit “HIPAA-ed out” because of the efforts they have already expended since HIPAA was enacted in 1996, particularly because of the past or current efforts to remediate their EDI Transactions. For others, the fact that the security compliance date is far into the future (2005) may give them a reason to pause.

However, many covered entities have already started the security assessment process, in some cases armed with the 1998 proposed security regulation, in order to get a head start on the effort. This assessment process should include both a gap analysis against the final security and privacy regulations and a risk assessment that is a requirement of the Final Security Rule. The security risk assessment will be the basis for decisions on how to best approach the “Addressable” implementation specifications.

Once the risk assessment and the 45 CFR Part 164 - security and privacy gap analysis have been completed - then a security and privacy strategy should be developed. As it relates to IAM, this strategy should consider the entire user lifecycle from the establishment of a digital identity, through the granting and changing of entitlements, and ultimately to access termination for these users.
The implementation of systems like Netegrity’s IAM solution should be coupled with the development and deployment of policies and procedures that will guide the implementation teams. IAM solutions will play a key role in helping organizations to meet the requirements of both the security and privacy regulations of HIPAA.

Conclusion

IAM solutions, like those available from Netegrity, will aid in timely and cost-effective implementations. If your organization is considered a covered entity under HIPAA, do not delay. If you have not begun to consider IAM solutions, start that evaluation process today.

In addition to meeting the specific requirements of HIPAA, there are other business drivers for the improvement of IAM processes in the healthcare industry, such as reducing costs, increasing efficiencies, increasing security to reduce risk, and improving the time it takes to deliver new applications and services to the various user communities. It is time to address the regulations and seize the opportunity for IT improvement through IAM solution implementation.
### Appendix

Table 1 - IAM Related Requirements from the HIPAA Final Privacy Rule & Netegrity’s Relevant IAM Functionality

<table>
<thead>
<tr>
<th>45 CFR Part 164 Standard</th>
<th>Associated Implementation Specification Required (R) or Addressable</th>
<th>Relevant Netegrity Functionality</th>
</tr>
</thead>
</table>
| **Minimum Necessary Requirements**  
A covered entity must meet the requirements (i.e., minimum necessary) with respect to a request for, or the use and disclosure of, PHI | **Minimum Uses of PHI (R)**  
1) A covered entity must identify: a) those persons or classes of persons, as appropriate, in its workforce who need access to PHI to carry out their duties and b) for each such person or class of persons, the category or categories of PHI to which access is needed and any conditions to such access; and 2) a covered entity must make reasonable efforts to limit the access of such persons or classes of persons to PHI. | Netegrity’s solution provides flexible role- and rule-based authorization mechanisms, so that access to PHI resources can be controlled, but provided to those whose job function requires it. |
| **Verification Requirements**  
Prior to any disclosure, a covered entity must verify the identity of a person requesting PHI and the authority of any such person to have access to PHI, if the identity or any such authority of such person is not known to the covered entity. | **Exercise of Professional Judgment (R)**  
The verification requirements are met if the covered entity relies on the exercise of professional judgment in making a use or disclosure or acts in good faith belief in making a disclosure. | Netegrity’s IAM solution provides centralized authentication and authorization services that are based on policies that management can institute to guide the user verification process. |
| **Access to PHI, Right of Access**  
An individual has a right of access to inspect and obtain a copy of PHI about the individual in a designated record set, for as long as the PHI is maintained in the record set | **Provision of Access (R)**  
If the covered entity provides an individual with access, in whole or in part, to PHI, it must provide the individual with access to the PHI in the form and format requested by the individual. | Because Web-based access through the Internet provides a more cost-effective and timely alternative to paper, the use of the Internet will grow as a method to meet this requirement.  
Netegrity’s IAM solution provides the authentication, authorization, auditing and reporting necessary to support Web-based access to PHI that is in line with the Final Privacy Rule. |
<table>
<thead>
<tr>
<th>45 CFR Part 164 Standard</th>
<th>Associated Implementation Specification Required (R) or Addressable</th>
<th>Relevant Netegrity Functionality</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safeguards</td>
<td>Safeguards (R) A covered entity must reasonably safeguard PHI from any intentional or unintentional use or disclosure that is in violation of the standards, implementation specifications or other requirements.</td>
<td>Netegrity’s IAM solution provides a centralized, policy-driven IAM system that can be used to administer and enforce access to systems and data, including PHI. This functionality can provide the due care required to meet this requirement.</td>
</tr>
</tbody>
</table>

A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of PHI.
Table 2 - IAM Related Requirements from the HIPAA Final Security Rule & Netegrity’s Relevant IAM Functionality

<table>
<thead>
<tr>
<th>45 CFR Part 164 Standard</th>
<th>Associated Implementation Specification Required (R) or Addressable</th>
<th>Relevant Netegrity Functionality</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Management Process</td>
<td>Implement policies and procedures to prevent, detect, contain, and correct security violations.</td>
<td>Information System Activity Review (R) Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.</td>
</tr>
<tr>
<td>Workforce Security</td>
<td>Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic PHI, and prevent those workforce members who do not have access from obtaining electronic PHI.</td>
<td>Authorization and/or Supervision (A) Implement procedures for the authorization and/or supervision of workforce members who work with electronic PHI or in locations where it might be accessed.</td>
</tr>
<tr>
<td>Workforce Clearance Procedure (A)</td>
<td>Implement procedures to determine that the access of a workforce member to electronic PHI is appropriate.</td>
<td>IdentityMinder functionality is designed specifically to address the challenges of user management, such as approval and notification related workflows. Once a user has their digital identity, whether it is a company officer, a business partner, an employee, or a casually interested customer, their access to corporate resources can be managed while safeguarding proprietary resources.</td>
</tr>
<tr>
<td>45 CFR Part 164 Standard</td>
<td>Associated Implementation Specification Required (R) or Addressable</td>
<td>Relevant Netegrity Functionality</td>
</tr>
<tr>
<td>--------------------------</td>
<td>------------------------------------------------------------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td><strong>Termination Procedures (A)</strong> Implement procedures for terminating access to electronic PHI when the employment of a workforce member ends or as required by determinations made as a result of other parts of the regulation.</td>
<td>Netegrity’s IAM solution provides an integrated workflow capability to manage user access and access removal requests efficiently.</td>
<td>IdentityMinder provides a flexible delegated user administration capability to effectively manage changes, suspensions and terminations of user access entitlements to PHI.</td>
</tr>
<tr>
<td><strong>Information Access Management</strong> Implement policies and procedures for authorizing access to electronic PHI that are consistent with the regulation.</td>
<td><strong>Isolating health care clearinghouse functions (R)</strong> If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic PHI of the clearinghouse from unauthorized access by the larger organization.</td>
<td>Netegrity SiteMinder provides centralized, policy-based authentication and authorization management for Web-based information &amp; applications, including digital PHI. This capability can be used both inside and outside a given organization.</td>
</tr>
<tr>
<td><strong>Access Authorization (A)</strong> - Implement policies and procedures for granting access to electronic PHI, for example, through access to a workstation, transaction, program, process, or other mechanism.</td>
<td><strong>Access Establishment and Modification (A)</strong> - Implement policies and procedures that, based upon the entity’s access authorization policies, establish, document, review, and modify a user’s right of access to a workstation, transaction, program or process.</td>
<td>Netegrity’s solution provides security and access management to systems based on policies that are built around the user and his/her relationship to the protected resource. The access can be made as granular as required.</td>
</tr>
<tr>
<td></td>
<td>The IAM solution from Netegrity provides fine-grained control over access through the creation of policies that can be used to manage individuals’ access to critical systems.</td>
<td>Also the processes and procedures for granting access to given resources can be implemented, monitored, and adjusted using the workflow capabilities of IdentityMinder.</td>
</tr>
<tr>
<td>45 CFR Part 164 Standard</td>
<td>Associated Implementation Specification Required (R) or Addressable</td>
<td>Relevant Netegrity Functionality</td>
</tr>
<tr>
<td>--------------------------</td>
<td>---------------------------------------------------------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>Security Awareness and Training Implement a security awareness and training program for all members of its workforce including management.</td>
<td>Log-in Monitoring (A) Procedures for monitoring log-in attempts and reporting discrepancies.</td>
<td>Significant auditing and reporting capabilities are built into Netegrity’s IAM solution to review users access privileges and how they have used those privileges. As an example, SiteMinder audits all user and site activity, including all authentications and authorizations, as well as administrative activity, and any changes to the policy store.</td>
</tr>
<tr>
<td>Password Management (A) Procedures for creating, changing, and safeguarding passwords.</td>
<td></td>
<td>Providing highly flexible user management capabilities, Netegrity’s IAM solutions manage the credentials by which people authenticate themselves. As an example, SiteMinder’s Password Services provide an additional layer of security to protected resources by enabling management of user passwords in LDAP user directories or relational databases. Key features include the automatic enforcement of password expiration, password composition, and password usage rules. Furthermore Netegrity’s Password Services can enforce multiple password policies through a priority list of passwords that apply to multiple applications being protected across one or more user directories. Password Services also enable password self-service and forgotten password services for end users.</td>
</tr>
<tr>
<td>Security Incident Procedures Implement policies and procedures to address security incidents</td>
<td>Response and Reporting (R) 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.</td>
<td>The detailed audit and monitoring capabilities built into Netegrity’s IAM solution provides the critical information to see where inappropriate access was attempted and occurred.</td>
</tr>
<tr>
<td>45 CFR Part 164 Standard</td>
<td>Associated Implementation Specification Required (R) or Addressable</td>
<td>Relevant Netegrity Functionality</td>
</tr>
<tr>
<td>--------------------------</td>
<td>---------------------------------------------------</td>
<td>---------------------------------</td>
</tr>
<tr>
<td>Access Control</td>
<td>Implement technical policies and procedures for electronic systems that maintain electronic PHI to allow access only to those persons or software programs that have been granted access rights.</td>
<td>IdentityMinder provides user self-service capabilities so that users can register themselves and create their own profile and request access privileges supported by an integrated workflow engine to ensure timely and accurate response to user requests for access privileges. Furthermore, IdentityMinder supports the creation of unique userids at the time of identity creation.</td>
</tr>
<tr>
<td>Unique User Identification (R)</td>
<td>Assign a unique name and/or number for identifying and tracking user identity.</td>
<td></td>
</tr>
<tr>
<td>Emergency Access Procedure (R)</td>
<td>Establish (and implement as needed) procedures for obtaining necessary electronic PHI during an emergency.</td>
<td>Using the Internet and Netegrity IAM solutions, access to PHI can be provided on a 24x7 basis from any Web-enabled system or workstation. With sufficient system architecture, zero down-time can be engineered into the system.</td>
</tr>
<tr>
<td>Automatic Logoff (A)</td>
<td>Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.</td>
<td>SiteMinder provides “automatic log-off” through its session management capabilities. This feature enables an administrator to control current user sessions, disable certain users and control user timeouts based on the sensitivity of the resource that they are accessing.</td>
</tr>
<tr>
<td>Audit Controls (R) - Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic PHI.</td>
<td>(none specified)</td>
<td>Netegrity’s IAM solution generates log files, which contain auditing information about the events that occurred within the system. This log can be printed in the form of several pre-defined reports, or customer-defined report formats, so that security events or anomalies can be analyzed and corrected. Alternatively this information can be configured to be loaded into a relational database to be used for further analysis.</td>
</tr>
</tbody>
</table>