

# Meeting HIPAA Standards for Information Security with Digital Guardian™

The HIPAA Security Rule requires health care providers, health plans and other organizations to protect against potential threats to the confidentiality and integrity of protected health information (PHI) in electronic formats. A companion to the HIPAA Privacy Rule, which spells out how protected data should be controlled, the Security Rule details a set of administrative, physical and technical safeguards designed to shield data from theft, abuse and misuse. Verdasys helps organizations meet their HIPAA compliance goals through an information security application that actively audits PHI use and enforces HIPAA policies across an enterprise.

## RISK ANALYSIS

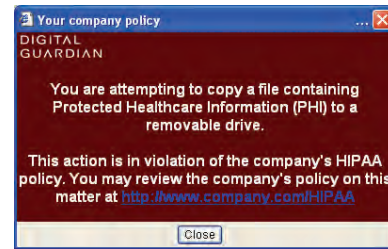
Digital Guardian automates the analysis of risks to PHI by tracking all application, file and network use and flow. Easy-to-interpret summary and trend reports reveal the vulnerabilities associated with the many unmanaged conduits of desktop information loss, such as e-mail, IM, USB flash drives, wireless interfaces, CD-ROMs and tunneled peer-to-peer networks. When more detailed analysis is required, fine-grained reports provide the information you need to develop informed security policies.

## RISK MANAGEMENT

Digital Guardian serves the central role in managing risks to PHI. While firewall and IDS products are designed to defend the external perimeter, Digital Guardian protects information at the application and data level from misuse by authorized users such as employees, contractors and partners, as well as hackers and unauthorized outsiders.

## Real-time Enforcement

Digital Guardian allows you to actively enforce policies governing the use of desktop applications, networks, and storage devices. Real-time response to violations can be as aggressive as the assessed risk demands.



## Application-Level Logging

Re-coding existing applications to support HIPAA can be both risky and expensive. Digital Guardian allows you to cost-effectively limit access to information without breaking open legacy applications and reworking the code, a time-consuming effort that may threaten business continuity and introduce new vulnerabilities.

## Data Redaction

Complying with HIPAA often requires organizations to “hide” data from employees who have access to enterprise applications but who are not authorized to view certain types of information. With Digital Guardian, you can control access to regulated data by blocking specific information from being viewed on screen by specific individuals – without complicated application re-coding.

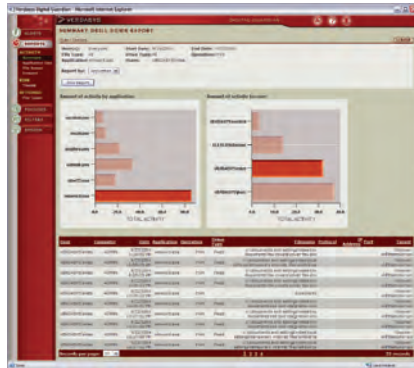
HIPAA Standard	Implementation Specification	Digital Guardian Feature
Management Process	Risk Analysis	<ul style="list-style-type: none"> <li>• Risk Trend Reports</li> <li>• Application, File &amp; Network Summary Reports</li> </ul>
	Risk Management	<ul style="list-style-type: none"> <li>• Real-time Policy Enforcement</li> <li>• Application-Level Logging</li> <li>• Sensitive Data Redaction</li> <li>• Adaptive Encryption</li> </ul>
	Sanction Policy	<ul style="list-style-type: none"> <li>• Real-time Administrative Alerts</li> <li>• Forensic Activity Reports</li> </ul>
	Information System Activity Review	<ul style="list-style-type: none"> <li>• Application, File &amp; Network Activity Reports</li> </ul>
Awareness & Training	Security Reminders	<ul style="list-style-type: none"> <li>• User Notifications &amp; Prompts</li> </ul>
Security Incident	Response & Reporting Procedures	<ul style="list-style-type: none"> <li>• Application, File &amp; Network Forensic Reports</li> </ul>
Audit Controls	Logging & Reporting	<ul style="list-style-type: none"> <li>• Application-Level Logging</li> <li>• Activity Trend &amp; Summary Reports</li> <li>• Application, File &amp; Network Activity Reports</li> </ul>

### Adaptive Encryption

To further minimize security risks, Digital Guardian can automatically encrypt information generated by applications that manage PHI as a response to centralized policy. This approach protects the confidentiality of information should it be accessed by an unauthorized party, and eliminates the need to train and rely on individual users for correct use of encryption technologies.

### SANCTION POLICY

Digital Guardian not only prevents misuse of PHI, but also gives you the information you need to implement HIPAA-based sanctions. Digital Guardian instantly



*Drill down pivot reports allow quick answers to who, where and how PHI has been accessed or modified throughout your organization.*

alerts compliance officers and security personnel to unauthorized actions and provides the evidence necessary to take immediate and decisive action against users who do not comply with policies.

### HIPAA AWARENESS & TRAINING

The success of the safeguards mandated by HIPAA is highly dependent on end-user awareness of policies. Digital Guardian continuously reinforces user understanding of HIPAA policies through customizable dialog boxes that can inform a user why an action has been blocked, display a prompt for a business justification before proceeding, or direct users to an intranet site or policy manual. This interactive policy enforcement provides the means to translate responsibility for compliance into individual user accountability.

### SUMMARY

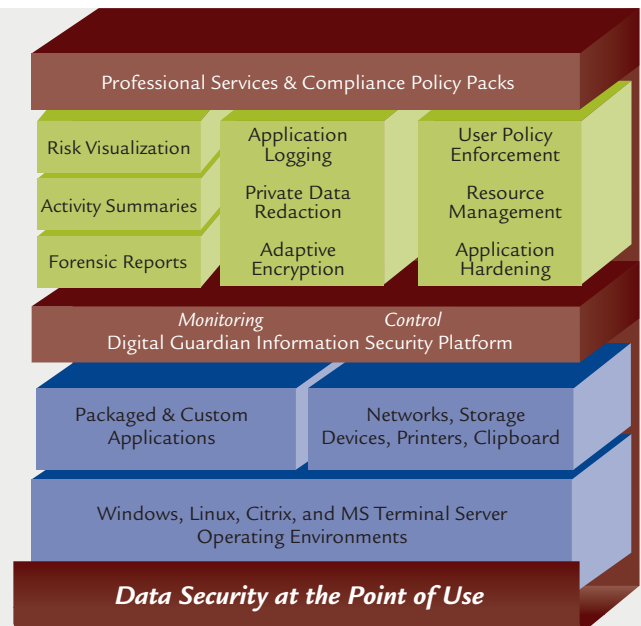
Digital Guardian gives you the tools you need to answer the question Who is accessing PHI, where is it and where is it going? By tracking all file and application access, storage and network activity and making the captured audit trail readily available, Digital Guardian reduces the considerable costs and administrative burden associated compliance reporting.

### VERDASYS INFORMATION SECURITY SOLUTIONS

Verdasys delivers information security solutions that address business-driven requirements for assuring compliance with a broad range of regulatory mandates; safeguarding the privacy of client and patient records; and preventing the misuse and theft of intellectual property.

Offering a compelling set of solutions for a wide array of data containment, global outsourcing and information protection challenges, the Verdasys Digital Guardian platform offers real-time, autonomous data-level monitoring and control. In addition to minimizing the information security risks posed by technologies such as e-mail, IM and USB drives, Digital Guardian detects and interdicts violations of information usage policies – thus creating a corporate culture centered on accountability.

Verdasys clients include Fortune 500 corporations – in industries ranging from insurance and financial services to multimedia and pharmaceutical – who are setting industry benchmarks for information security. To join them, contact us at [compliance@verdasys.com](mailto:compliance@verdasys.com)



### VERDASYS.

950 WINTER STREET, SUITE 2600 WALTHAM, MA 02451  
781-788-8180 TEL 781-788-8188 FAX  
COMPLIANCE@VERDASYS.COM WWW.VERDASYS.COM