



A Websense® White Paper

Using Data Loss Prevention For Health Care Compliance

How Data Loss Prevention (**DLP**) Technology can **Protect** Electronic Patient Health Information (**ePHI**) and Address Requirements of the Health Insurance Portability and Accountability (**HIPAA**) and Health Information Technology for Economic and Clinical Health (**HITECH**) Acts

websense®
ESSENTIAL INFORMATION PROTECTION™

Disclaimer: This white paper is not intended to provide legal guidance on HIPAA or HITECH Act compliance. If you have questions about the meaning of a particular provision of HIPAA or its implementing regulations or of the HITECH Act or its implementing regulations, you should consult your attorney. The Websense® data loss prevention product suite is a tool that people can use to help them comply with these requirements, but it is not a regulatory compliance product and will not guarantee that a given business practice is compliant with particular laws or regulations. Nothing in this whitepaper is intended to, or does, provide any warranty regarding the Websense products. Each product is subject to an agreement that contains certain contractual terms and conditions that govern its use. You are encouraged to evaluate the Websense products and make your own determination as to the suitability of the products for your needs.

Table of Contents

Executive Summary.....	3
Protecting ePHI: Drivers and Challenges.....	4
It all started with HIPAA.....	4
New risks in the movement from paper to electronic records.....	4
The HITECH Act: Unprecedented influence over ePHI security.....	5
Other applicable regulations.....	7
How is ePHI Being Used?.....	8
The Optimal Data Loss Prevention Solution Offers Visibility and Control Over ePHI..	9
Visibility.....	9
Visibility through coverage for ePHI usage scenarios.....	9
Visibility into content for efficient detection of patient ePHI.....	9
Enterprise email is legitimate, but its use may not be.....	10
Web traffic can mean any traffic and more risks for data loss.....	10
SSL does not mean ePHI is secured.....	10
End-user systems shouldn't be a compliance black hole.....	10
Stored data may not just be "resting".....	10
Control.....	11
Avoid disclosure costs through automated encryption.....	11
Avoid disclosure by avoiding breach in the first place.....	11
Keeping systems "clean" by controlling Web access.....	11
Manage policies and reporting to demonstrate compliance.....	11
Websense Data Loss Prevention: A means to protect ePHI.....	13
Websense® Data Security Suite.....	13
Policy templates for effective detection of ePHI content.....	13
Granular policy engine helps address compliance and business rules.....	14
Dashboards and reporting for efficient compliance management.....	14
Websense Data Monitor.....	15
Visibility into SSL traffic.....	15
Blocking access to malware-hosting Web sites.....	15
Websense Data Protect.....	15
Automated encryption of emails containing ePHI.....	15
Block unauthorized email or Web transmission of ePHI.....	15
Block unauthorized upload of ePHI over SSL-encrypted Web sites.....	15
Websense Data Endpoint.....	16
Endpoint visibility and control.....	16
Endpoint discovery and data classification.....	16
Websense Data Discover.....	16
Network discovery and classification.....	16
Automated enforcement of stored data.....	16
Conclusion.....	17
Appendix: Health Care Regulation Mappings.....	18

Executive Summary

New legislation for the security of electronic Protected Health Information (ePHI) and increased movement towards electronic medical records (EMR) and electronic health records (EHR) have considerably increased the scope and relevance of the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, forcing providers to revisit their current procedures. EMR is increasing the availability of patient records in electronic format, which calls for increased scrutiny of common business productivity applications.

While EMR increases the scope of HIPAA to newly digitized records, the Health Information Technology for Economic and Clinical Health (HITECH) Act may just be the catalyst for stricter enforcement of the HIPAA Security Rule, which previously were not considered with much urgency. The Act imposes strict new disclosure requirements when “covered entities” discover possible security breaches involving unsecured ePHI — and allows for exemptions when these breaches pertain to encrypted or secured ePHI. The Act also extends HIPAA requirements to business associates processing ePHI on behalf of covered entities and imposes additional audit requirements for ePHI disclosure.

Organizations subject to the HITECH Act and the HIPAA Security Rule must facilitate the business of health care while minimizing risks associated with unauthorized disclosure of ePHI. Key questions they will need to answer include:

- How would it be known that an ePHI breach has occurred?
- How could a breach be prevented?
- If a breach does occur, even if it were the result of a legitimate business process, albeit with unsecured data, could that business process be secured to prevent future breaches?
- If there is an audit, will there be a way to demonstrate an audit trail of all ePHI disclosure instances?

Data Loss Prevention (DLP) solutions are essential to compliance with these requirements but must exhibit the following key attributes. They must:

- **Provide visibility** into ePHI content across multiple usage scenarios including email, Web, endpoint applications, peripheral storage, and enterprise storage systems. This helps satisfy many HIPAA security rule and HITECH Act requirements for ePHI disclosure by detecting breaches as they occur.
- **Exert control** by enforcing encryption of ePHI in common business processes such as email and storage in databases. Prevent the breach in the first place by blocking its transmission via email and Web, or block copy from end-user applications to peripheral devices. Simplify enforcement using policy templates and reporting, which is both built in and customizable.

The Websense® data loss prevention product suite covers **all** of these ePHI usage scenarios through a single, unified solution that offers built-in policies for visibility and control over ePHI.

Protecting ePHI: Drivers and Challenges

It all started with HIPAA

With over ten years having passed since its enactment in 1996, HIPAA holds the distinction of providing the first federal standards to protect individual medical records and enable ready access to these records by patients and their health care providers. According to the U.S. Department of Health and Human Services (HHS) HIPAA Security Rule from 2003, “covered entities”ⁱⁱⁱ are required to employ safeguards that “ensure the confidentiality, integrity, and availability of all electronic protected health information (PHI)” (§ 164.306(a)(1)) under their control.ⁱⁱⁱ PHI primarily covers the patient’s personally identifiable information (PII) such as their name, Social Security number (SSN), ethnic background and/or address *in conjunction* with any of the following: FDA National Drug Codes (NDC), DNA profiles, diseases, and other health care information.

Breach disclosure: HIPAA also required covered entities to enter into contracts with business associates (HIPAA Security Rule § 164.308(b)(1)), such as entities that provide services such as record storage or payment processing, to safeguard PHI being processed by that business associate on behalf of the covered entity. These requirements were enforced only through contractual obligations, as opposed to regulatory oversight.^{iv}

Policy training: For most organizations, HIPAA compliance is acknowledged at minimum through implementation of periodic workforce member training on HIPAA policies and procedures (§ 164.308 (a)(5)(i) for Security awareness and training and § 164.308 (a)(6) for policies). Implementation of automated controls varies depending on awareness as well as volume of electronic patient records.

Additional safeguards: For more technologically advanced organizations, implementation of safeguards to address the HIPAA Security Rule may include access control (§ 164.312(a)(1)), malware protection (§ 164.308 (a)(5)(ii)(B)) risk management (§ 164.308 (a)(1)), device and media controls (§164.310(d)(1)), transmission security (§ 164.312(e)(1)), and minimizing sensitive data collection (§ 164.514(d)). These requirements not only present challenges to IT operations but also to end-user usability.

New risks in the movement from paper to electronic records

Arriving with the new millennium were initiatives to reduce paper records for cost and environmental reasons, but also to facilitate easier access to patient data — presumably in support of the “portability” goal of HIPAA. With EMR systems, providers can more easily share data with their patients, as well as with other providers, through standard means such as email, Web portals, and applications with access to patient records databases. This initiative brings its own challenges, though, since EMR systems don’t come without cost, such as scanning or manual transcription of existing paper records into electronic format, EMR projects (evaluation, selection and deployment of solutions), and personnel training.

With EMR challenges come new areas of risk as well. ePHI is now available for access by providers from general purpose computing systems, such as desktops and laptops. Even with data being secured through access control on EMR applications, authorized users can copy and download data from client/server applications, patient health care portals, and databases. Once this data is in the possession of the authorized user, that user may transport this data via email, Web applications, and USB storage devices. In other words, while ePHI data loss risks existed in the world of paper records, electronic records have dramatically increased these risks. And with recent U.S. government funding for qualified health care organizations to implement EMR systems, these migrations may happen sooner than later.

The HITECH Act: Unprecedented influence over ePHI security

In February 2009, the American Recovery and Reinvestment Act (ARRA) was signed into law, with a \$787 billion economic stimulus plan to fund various initiatives such as tax cuts, social welfare, and spending in education, infrastructure, energy, and health care. The Health Information Technology for Economic and Clinical Health (HITECH) Act allocates \$19 billion of the ARRA provisions to promote seamless and secure exchange of information as a means to deliver higher quality, lower cost health care services.^v While these funds (some allocated for EMR initiatives) will phase in over a period of several years, most of the security and privacy-related provisions in the HITECH Act will take effect on February 17, 2010.^{vi}

Beyond the additional funding and deadlines for health care modernization, the HITECH Act extends certain HIPAA requirements to business associates, mandates disclosure of unsecured PHI data breaches, exempts secured PHI from these disclosure requirements, and requires audit trails of PHI data disclosures. And given the steady adoption of EMR technology and widespread use of electronic business productivity applications in the business of health care, PHI can be regarded as ePHI – or Electronic Protected Health Information.

Extend HIPAA Requirements to Business Associates

The Act extends certain requirements of HIPAA to “business associates” of health care providers, such as the security rule. This means that business associates must secure ePHI and be subject to breach disclosure requirements as well. The requirements also extend beyond “workforce member” to “workforce member,” covering “workforce members, volunteers, trainees,” and others who work on behalf of a covered entity.

While this is good news for patient privacy, health care providers may be challenged with enforcing their ePHI data protection policies with their business associates, once the data has been transmitted from the provider network.

Breach Disclosure Requirements

The HITECH Act (HI TECH § 13402) specifically imposes strict new disclosure requirements when “covered entities”^{vii} discover possible security breaches involving unsecured PHI. “Unsecured PHI” includes protected information that is “not secured through technology or methodology.” The “timeliness, content, and methods of providing breach notifications”¹ are further detailed in §164.404 Notification to individuals. Timeliness and content in particular are within the control of IT departments and some data owners, while “methods” focus on external communication with patients, the HHS, and if necessary, media outlets.

Timeliness: Once a breach is discovered, the covered entity must notify the affected patients (and where applicable, the HHS) “without unreasonable delay, but no later than 60 days” after the breach was discovered.² If the data breach incident involves more than 500 individual records in a particular jurisdiction, the health care provider must notify the media about the incident. These same requirements are extended to the Federal Trade Commission (FTC) for vendors of personal health records (PHRs). The only exception to this time limit is for § 164.412, where “notification would impede a criminal investigation or cause damage to national security, and specifies the time for which a delay is required.”

Content: The Act requires that disclosure include “a brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known.” It also asks for the specific ePHI that was involved in the breach, including “full name, Social Security number, date of birth, home address, account number, diagnosis, disability code, or other ...”

¹Page 42741, “Interim Final Regulations”

²Page 16 Federal Register, vol. 74, no. 162 (Aug. 24, 2009), “45 CFR Parts 160 and 164 Breach Notification for Unsecured Protected Health Information; Interim Final Rule”

But compliance is not without cost, considering credible estimates^{viii} of \$5.89 per affected individual (e.g., email/mail notification, toll-free hotlines, notice to HHS/media, etc.). Since data breach incidents routinely involve hundreds of thousands of individual records, the potential costs associated with unsecured PHI could impose a massive burden on health care providers.

Allowing up to 60 days from breach discovery to notification may seem reasonable on the surface, but the damage may well have already been done with these types of delays. In some cases, a patient may discover the breach on their own and in other cases the media may discover the breach.

Discovery outside of health care provider purview can be extremely damaging to the reputation of the provider. The inability to proactively detect ePHI data breaches increases the risk of non-compliance and reputation damage.

Disclosure Exemptions

“Encryption is, in practice, the only technology that allows health care providers to claim a “safe harbor” exemption in the event of a PHI data breach incident.”^{ix} - The HITECH Act of 2009

While unsecured PHI is subject to breach disclosure requirements, secured PHI is explicitly mentioned as being exempt from these requirements. “Secured PHI” is defined as protected information that is either encrypted or destroyed — an important distinction for determining the scope of breach disclosure requirements for both data owners and IT operations.

Gaining some breathing room on breach disclosure requirements would be a significant benefit to providers who regularly engage in common business activities such as email and access to patient records databases. Minimizing the impact of a data breach by enforcing encryption in business activities could greatly reduce impact on IT operations and PHI data guardians in the event of a breach. But this is easier said than done since widespread encryption of all stored and transmitted data is impractical, costly, and difficult to manage. Also impractical is expecting end-users to identify and encrypt ePHI. The ability to automatically encrypt ePHI data alone is essential for practical implementation.

Auditing Guidelines

Covered entities will be subject to audits that may require them to document where, when, how, and to whom protected electronic records have been disclosed. In addition to maintaining activity logs and other audit-trail documentation for regulatory compliance purposes, patients may require providers to account for any disclosures of their medical records during the previous three years.

These audit requirements place considerable burden on providers given that ePHI is stored, used, and transmitted in so many different ways. Email and Web, specific business applications on end-user systems, peripheral storage devices, and access to enterprise systems such as databases and file servers all create opportunities for efficient access to information. But these same tools can also be used to leak ePHI to unauthorized locations or recipients. Since the audit requirements are concerned with ePHI data disclosure, regardless of how it is being handled, audit solutions must also provide coverage for these different areas.

Other applicable regulations

Compliance in health care may start with HIPAA, but it certainly doesn't end there.

In addition to related industry regulations, health care providers are also subject to the laws of their region, as in the case of state privacy laws, which have recently accelerated efforts to formally require protection of individual data including financial and health care.

In 2003, California became the first state to require businesses to disclose any incident involving the unauthorized disclosure of unencrypted personal information.^x Since then, more than 40 states have adopted similar laws, compelling national health care providers to address an increasingly complex mosaic of state and federal health care privacy regulations.

Other industry regulations may spill over into health care organizations as well, as in the case of the Payment Card Industry Data Security Standard (PCI DSS), which oversees the protection of credit card data. From medical facilities to hospital gift shops, credit cards are used as payment for goods and services, making these health care providers liable for the protection of cardholder data.^{xi}

How is ePHI Being Used?

WHIPAA puts the spotlight on confidentiality, integrity, and availability of ePHI without specifics on implementation requirements. But proactive health care providers have asked themselves the right questions to determine HIPAA compliance, especially in the area of confidentiality:

- Where is my ePHI stored, and what is being done to secure its use and transmission?
- What are my users doing with this data when they are on the enterprise network? Do I know what they're doing with this data when they are remote or mobile?

The HITECH Act requirements augment existing HIPAA guidelines with increased focus on data breach scenarios, leading providers to ask:

- How would it be known that an ePHI breach has occurred?
- How could a breach be prevented?
- If a breach does occur, even if it was the result of a legitimate business process, albeit with unsecured data, could that business process be secured to prevent future breaches?
- If there is an audit, will there be a way to demonstrate an audit trail of all ePHI disclosure instances?

These questions all point to the need for understanding ePHI usage scenarios, which in most enterprises includes common business activities. Workforce members upload confidential data to social networking sites and email unencrypted, confidential data to partners. The problem of data loss is exacerbated by the increase in mobile computing, the widespread use of peripheral storage devices, and easy access to client software with file download and file-sharing capabilities.

Email: Workforce members of covered entities communicate amongst themselves but also with insurers and in some cases, patients, with sensitive data such as medical diagnosis or prescription information. Authorized but unsecured (unencrypted) email is prone to eavesdropping. Unauthorized emails — encrypted or not — can result in ePHI falling into the wrong hands.

Web applications: ePHI could be uploaded to unauthorized locations by users with unrestricted use of the Web, such as via webmail, online storage, and social networking sites. Sometimes webposts are done over secured channels such as SSL, but this does not mean that only authorized users are posting and accessing ePHI over the Web.

Mobility and end-user applications: Users travel with laptops which may contain ePHI downloaded from EMR applications and patient databases. Use of peripheral storage devices is suitable for personal and acceptable business use but also creates risk of ePHI storage on unsecured devices.

Storage: Patient data is stored in obvious places such as databases but also in places one would not expect (user desktops, laptops, file servers). ePHI is also routinely updated — both due to business process but sometimes due to tampering.

The Optimal Data Loss Prevention Solution Offers Visibility and Control Over ePHI

Data Loss Prevention (DLP) solutions have been considered by some health care providers as a necessary means for compliance with HIPAA, the HITECH Act, and other regulations protecting ePHI or other confidential data. As the name suggests, preventing leaks from occurring in the first place is an effective means for securing confidential data. The HITECH Act in particular highlights the obligations of covered entities in breach disclosure, because this would result in the most severe violation of patient privacy.

But point solutions with limited coverage over ePHI usage scenarios have resulted in spotty adoption. DLP solutions are essential to compliance but must offer **visibility and control** over how ePHI is being handled across common business process. And while addressing compliance, covered entities must also keep an eye on operational expenses due to managing point solutions and training personnel.

Visibility

Securing ePHI is only possible through visibility into the data itself and into all places where data lives, moves, and is used.

Visibility through coverage for ePHI usage scenarios

Wherever an end-user or automated process has access to ePHI is where a data breach can occur. Focusing exclusively on one area — such as database — cannot ensure sufficient visibility across common usage scenarios. The DLP solution must therefore cover a wide range of ePHI usage scenarios to determine where it is being transmitted, used, and stored. Email, Web, endpoint EMR applications, peripheral storage and enterprise storage systems are commonly used in business processes and for personal use.

This coverage also helps address the “timeliness” requirements for breach disclosure in the HITECH Act, since the more places being monitored means earlier warning on a possible data breach, and faster response time for disclosure.

Visibility into content for efficient detection of patient ePHI

Compliance with regulations governing protection of ePHI requires accurate detection and classification of the content. Covered entities must be able to identify personally identifiable information (PII) along with health care information such as medical diagnosis and drug codes.

Taking this one step further, to avoid unnecessary alarms for every case where ePHI is detected, the organization should keep current snapshots of ePHI for which they are guardians. In other words, a health care organization workforce member may send their personal medical diagnosis information via email or Webmail to a family member with an external address, but this should not necessarily trigger a breach notification response. Unless this workforce member also happens to be a patient of this organization, this data may not constitute an actual breach.

Visibility into content helps address the “content” requirements for breach disclosure in the HITECH Act, with details into the ePHI detected, the specific patients affected, date/time of the breach, and how the data was leaked.

Enterprise email is legitimate, but its use may not be

Workforce members in a health care organization communicate internally and with external providers, insurers—and in some cases, patients using IT-supported email services. While the use of email for communicating ePHI with authorized recipients is a valid use of the service, it also creates risk of a data breach in cases where the ePHI is sent in the clear, either through file attachments or as part of the message body. Any reasonably capable hacker could intercept these communications and view/modify sensitive patient data, violating HIPAA rules for confidentiality and integrity and triggering HITECH Act rules for breach disclosure. In other cases, email may also be used to send ePHI to unauthorized recipients, violating HIPAA rules for access control as well as triggering the HITECH Act rules for breach disclosure.

Email is also a key vector for populating data stores with confidential information, since ePHI may be sent and received via email and stored on email servers and local email clients.

Web traffic can mean any traffic and more risks for data loss

While email is an IT-sanctioned application, the reality of business in today's world is that Web access is expected by end-users. But IT may not be able to control where users go on the Web, and it is no longer true that Web is truly just Web traffic. Users routinely access Web mail for personal email services and in recent years, access to social networking sites has jumped, making it easier to post content in one place, and have thousands of "friends" or "followers" view this information.

Adding to the IT security challenge are countless applications that can be "tunneled" (or hidden) within the HTTP protocol, such as instant messaging. The vast number of public Web sites combined with the likelihood that applications go beyond simple HTML (e.g., Java Script and XML) creates tremendous risk of an ePHI data breach.

SSL does not mean ePHI is secured

Many Web sites support SSL — although SSL maintains confidentiality of the communication, it can also be used to evade controls over unauthorized ePHI access. The inability to inspect SSL traffic casts a shadow of doubt over HIPAA compliance due to lack of visibility into commonly used secure Web channels. Consider the authorized user who downloads patient records and then uploads this information to easily accessible secure storage sites such as Google docs and Drop Box. These sites may enable secure transmission of ePHI across public networks, but they do not enforce access control since any user outside of the covered entity could have access to these destinations.

End-user systems shouldn't be a compliance black hole

Even the more advanced organizations rely exclusively on network security controls to protect ePHI, leaving a major area of risk open — the end-user systems (desktops, laptops). Users may have privileged access to ePHI data when on the network and can download data to their systems from EMR applications, databases, emails, and file servers. This data could be copied to peripheral storage devices and even worse, once they are away from the corporate network, they could use any number of applications to transmit ePHI to unsecured locations. Keeping inventory of ePHI stored on end-user systems and preventing copy and transmission of this data from the system is essential to closing this common compliance gap.

Stored data may not just be "resting"

Much is said about data at rest and the importance of taking inventory of confidential data such as ePHI to identify all critical assets. This is indeed essential for effective breach disclosure, not just for visibility into patient records but also to identify where data is stored in the clear (unencrypted), if it has been modified/removed/added since the last audit, and if the file permissions are set to only allow authorized access. End-users and applications update stored data in databases, files servers, and email storage servers, making this data very much alive and requiring periodic discovery to update its inventory. Visibility into stored data is key to enforcing HIPAA rules for confidentiality and integrity of ePHI. Regular inventory of these data stores goes further to address HIPAA security risk management requirements.

Control

Gaining visibility into ePHI where it lives, moves, and is used further enables compliance but also creates obligation for the covered entity to protect the data in these scenarios. One method of protection is to make the confidential data unreadable by unauthorized users, with the use of encryption technology for transmitted data (over email) and for stored data (file servers, databases). Another method of protection is to block its transmission via email and Web, or block copy from end-user applications to peripheral devices.

Avoid disclosure costs through automated encryption

Uncovering the transmission of unsecured ePHI over email is a certain data breach but given that many of these breaches are inadvertent and intended for legitimate use requires control that is:

- Intelligent enough to **monitor and detect** ePHI over email.
- Able to determine if the sender and recipient are **authorized** to view the content.
- Able to automatically **encrypt** the email communication if it is for legitimate use.

This level of control not only enables legitimate business use of email for sharing ePHI but also avoids the certain expense and embarrassment associated with disclosing a data breach.

Unsecured ePHI stored on centralized storage systems such as databases, file servers, and email servers is a certain risk for data breach even if authorized users access the information. Once this data is downloaded onto end-user systems, it could be copied to peripheral storage devices and network locations using email and Web applications. Encrypting stored data is therefore another safeguard to avoiding breach disclosure requirements while honoring the HIPAA confidentiality requirements.

Avoid disclosure by avoiding breach in the first place

With all the details on breach disclosure requirements, it should not be forgotten that if possible, avoidance is the best safeguard. Blocking unauthorized email, Web upload, and end-user copy of ePHI is a preventive control, which not only helps avoid the HITECH Act breach disclosure requirements but also enables targeted policy education for repeat offenders.

For email, the sender can be both notified and blocked from sending ePHI to an unauthorized recipient. For Web traffic, allowing access to social networking Web sites can be fine but posting ePHI data should be blocked. Similarly, end-users who copy personal or non-confidential business information to USB storage devices can continue to do so, but if an EMR application is accessed and ePHI is copied to this external storage, it should be blocked.

Keeping systems “clean” by controlling Web access

The Web continues to be the primary vehicle to deliver malicious software to end-users, which then opens up back doors for hackers to remotely access systems or sends end-user data to remote sites. For covered entities where users have privileged access to patient data, keeping systems free of malware is not only essential to prevent an ePHI data breach but also to comply with the HIPAA rules to protect against malicious software.

Manage policies and reporting to demonstrate compliance

Keeping pace with the various ePHI data types that are in scope for HIPAA compliance, such as PII and drug codes, is time consuming, and if not done properly, can result in ePHI identification that is inaccurate or absent. Add to this the various regional and industry regulations, such as state privacy laws and credit card security through PCI DSS, and you have operational challenges that put compliance at risk. Monitoring for confidential data has to be reconciled with the various usage scenarios as well, since authorized users may be allowed to handle ePHI in certain ways while other users should be prevented from most actions involving ePHI. For covered entities with relatively small IT organizations and a limited budget, addressing these issues can seem like a difficult choice between health care compliance and business viability.

Policy templates: Current policy templates that are supported by a trusted provider can help accurately detect any data types (e.g., structured for databases, unstructured otherwise) and determine if the data contains ePHI or other confidential data. Consistent and accurate detection of all regulated data is a key requirement for DLP solutions.

Granular policy engine: Covered entities need to reconcile health care regulation requirements within their own organizations and as such, require the ability to specify who, what, where, and how ePHI can be handled by end-users. A granular policy engine should enable implementation of business rules that honor health care regulations.

Dashboards, reporting, and alerts: With the volume of activity over numerous usage scenarios, IT administrators need a scalable way to monitor ePHI activity. Real-time dashboards and historical reports showing ePHI activity over these usage scenarios are necessary for ongoing policy refinement and compliance reporting. Alerting mechanisms such as email and logging are also essential.

Websense Data Loss Prevention: A means to protect ePHI

The combined challenges of industry regulations and ready access to confidential data through electronic means highlights the need for streamlined DLP solutions in health care institutions. Websense helps address these challenges with a complete DLP suite to identify, monitor, and protect confidential data across the network, on user desktops and laptops, and in network data repositories.

Websense® Data Security Suite

Websense® Data Security Suite provides the necessary coverage and manageability across common ePHI usage scenarios, the accuracy and depth of point solutions, and the advantage of a single-policy framework. The Data Security Suite helps organizations comply with regulations like HIPAA and the HITECH Act with its built-in content classifiers that inspect business communications and stored documents for ePHI and other confidential data — on the network, on end-user systems, and on enterprise storage systems.

Policy templates for effective detection of ePHI content

The solution comes with built-in classifiers and customizable templates for the detection of health care confidential information with PII including:

- Credit Cards and Sensitive Disease or Drug Information
- Credit Cards and Common Diseases
- DNA Profile (stand alone or in proximity to related terms)
- DOB (Date of Birth) and Name
- ICD10 (International Statistical Classification of Diseases) Codes
- ICD10 Code + Description
- ICD10 Codes + U.S. full names
- ICD10 Descriptions + U.S. full names
- Names and Common Diseases (stand alone or in proximity to related terms)
- Names and Sensitive Disease or Drug (stand alone or in proximity to related terms)
- NDC (National Drug Codes) Number (stand alone or in proximity to related terms)
- SSN and Sensitive Disease or Drug Information
- SSN and Common Diseases

The screenshot displays the Websense Policy Screen. On the left, a tree view shows various policy categories such as Credit Cards, Customer Information, and HIPAA. The 'HIPAA' category is expanded, showing sub-policies like 'HIPAA: SSN and Sensitive Disease or Drug', 'HIPAA: SSN and Common Diseases', etc. On the right, the 'Policy: HIPAA' is selected, showing its description and a list of 13 rules. The rules are numbered and include details such as the rule name, description, and status (e.g., 'Enabled', 'Disabled').

Policy: HIPAA

Description: The Health Insurance Portability and Accountability Act is a US Federal law that specifies a series of administrative, technical, and physical safeguards, organizational and documentation requirements for covered entities to use to assure the availability, confidentiality, and integrity of electronically protected health information. The policy detects combinations of Personally Identifiable Information (PII) like name, social security or credit card number, and sensitive health information such as diseases.

Rules (enabled: 12, total: 17)

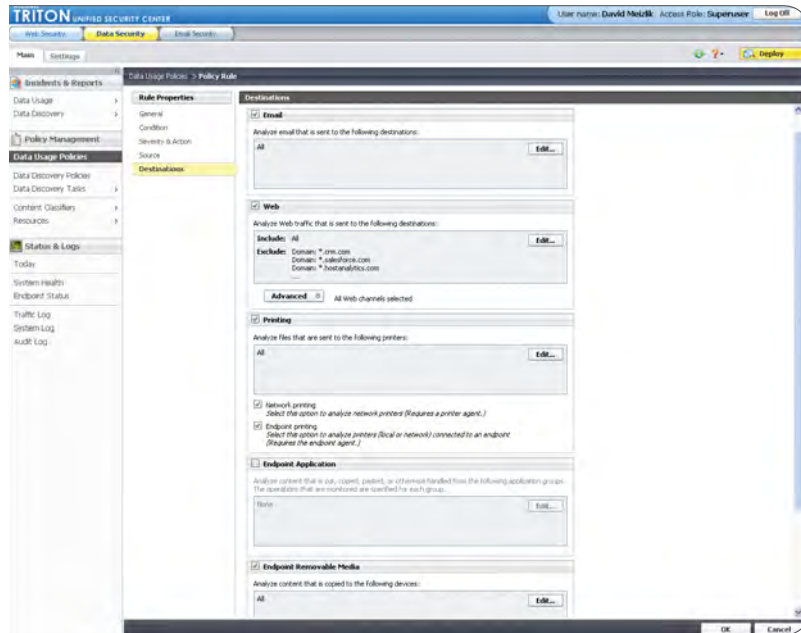
- HIPAA: SSN and Sensitive Disease or Drug**
Rule for detecting valid social security numbers that have been issued by the US Social Security Administration, when appearing together with the name of a disease, drug or a medical condition which is of a sensitive nature.
- HIPAA: SSN and Common Diseases**
Rule for detecting valid social security numbers that have been issued by the US Social Security Administration, when appearing together with name of a common disease or health issue.
- HIPAA: Credit cards and Sensitive Disease or Drug**
Rule for detecting any valid credit card number prevalent in the US, employing various heuristics involving credit card related terms and use of delimiters, when appearing together with the name of a disease, drug or a medical condition which is of a sensitive nature.
- HIPAA: Credit cards and Common Diseases**
Rule for detecting any valid credit card number prevalent in the US, employing various heuristics involving credit card related terms and use of delimiters, when appearing together with a name of a common disease or health issue.
- HIPAA: Names and Common Diseases**
Predefined NLP rule for detecting a combination of US full name in proximity to the name of a common disease or health issue.
- HIPAA: Names and Sensitive Disease or Drug**
Predefined NLP rule for detecting a combination of US full name in proximity to the name of a disease, drug or a medical condition which is of a sensitive nature.
- HIPAA: DNA profile (default)**
Rule to detect DNA profiles (strings composed of A,C,G,T).
- HIPAA: DNA profile (override)** - Disabled
Rule to detect DNA profiles (strings composed of A,C,G,T) when appearing in proximity to names terms. This rule is user-selectable by default.
- HIPAA: DOB and Name**
Predefined NLP Rule for detecting Name in proximity to Date of Birth.
- HIPAA: NDC numbers (default)** - Disabled
Rule for detecting National Drug Code (NDC) numbers of prescription drugs in insulin products. All insulin products in the database are further than 20 years. This naming issue this mechanism is not affected by default.
- HIPAA: NDC numbers (override)** - Disabled
Rule for detecting National Drug Code (NDC) numbers of prescription drugs in insulin products. Underlined numbers are passed a manual validation.
- HIPAA: NDC numbers (override)** - Disabled
Rule for detecting National Drug Code (NDC) numbers of prescription drugs in insulin products. All insulin products in the database are further than 20 years. This naming issue this mechanism is not affected by default.
- HIPAA: ICD10 Codes**
Predefined NLP rule for detecting at least 10 codes that belong to the ICD10 system. No additional information is required.

Policy Screen Showing Ability to Customize Policies

For organizations that need specialized detection policies, these templates can be use as a baseline so that ePHI data owners can add or remove rules as needed. Administrators can use dictionaries, keywords, regular expressions, and fingerprinted data from actual patient data stores to further refine policies.

Granular policy engine helps address compliance and business rules

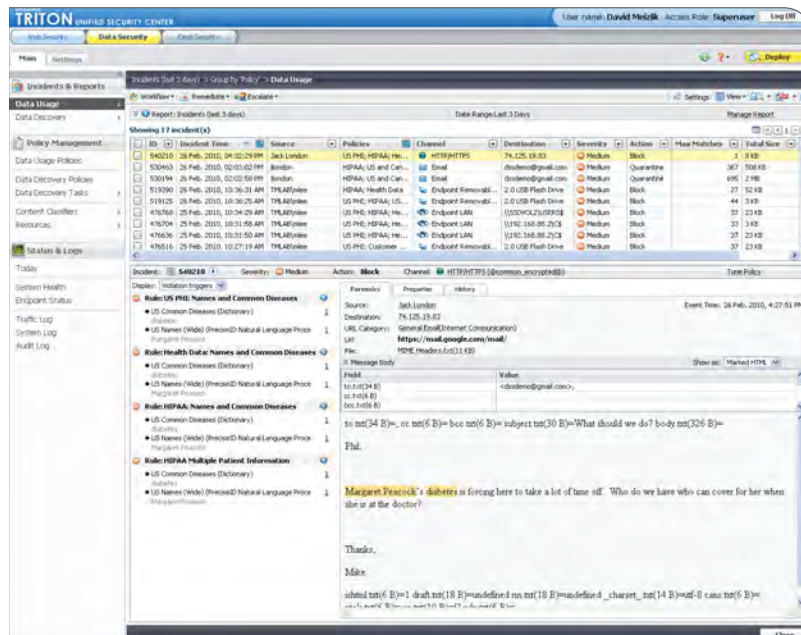
In addition to the time-saving policy templates, Websense Data Security Suite provides a customizable policy engine, which allows administrators to monitor and protect ePHI across email, Web, endpoint, and data storage usage scenarios. Within these scenarios, more detail such as files types, user identification, Web destinations, and file permissions can be specified.



Policy Screen Showing Sules for Email Sender and Web Destination

Dashboards and reporting for efficient compliance management

For visibility across all usage scenarios, both in real time and for historical reporting, Websense provides a built-in dashboard and numerous pre-defined reports for simplified management of HIPAA and HITECH Act compliance.



HIPAA Incident

The Websense® Data Security Suite comprises four modules — each deployable alone or jointly — for flexible enforcement by HIPAA-covered entities and their business associates:

- [Websense Data Monitor](#)
- [Websense Data Protect](#)
- [Websense Data Endpoint](#)
- [Websense Data Discover](#)

Websense Data Monitor

Websense® Data Monitor is a DLP solution for network applications such as email and Web, providing visibility into ePHI and context into what patient data is being leaked. Administrators can see if unsecured ePHI is being emailed on a regular basis, allowing them to focus training efforts on legitimate use of email. Similarly, attempts to transmit ePHI using webmail or social networking Web sites can also be detected. This means more actionable alerts and less effort for administrators to address HIPAA and HITECH Act violations.

Visibility into SSL traffic

Websense allows for monitoring of encrypted SSL traffic (without the need for a third-party solution) to ensure that even if the data is obfuscated as it is sent over the network, that it is still visible for the purpose of HIPAA and HITECH Act compliance.

Blocking access to malware-hosting Web sites

Websense enables DLP monitoring with visibility into specific Web destinations known to be hosting malicious software. By blocking end-user access to these Web sites, endpoints where EMR applications or ePHI data are stored are less at risk for being hacked.

Websense Data Protect

Websense® Data Protect includes all monitoring features of Websense Data Monitor but goes further to include enforcement controls over network activity such as email and Web.

Automated encryption of emails containing ePHI

Rather than rely on end-users to make note of confidential content and enforce encryption before sending to an authorized recipient, these actions can automatically be enforced. By simplifying the method to secure ePHI over email, covered entities can avoid HITECH Act breach disclosure requirements and enforce HIPAA requirements to maintain confidentiality of ePHI.

Block unauthorized email or Web transmission of ePHI

In other cases, ePHI should never be transmitted — whether it is encrypted or not. Posting to social networking sites, sending via webmail, or using enterprise email to send ePHI to unauthorized recipients are all activities that should automatically be blocked. By doing this, the data is never actually leaked, so the breach has been avoided.

Block unauthorized upload of ePHI over SSL-encrypted Web sites

Workforce members may be authorized to post patient data to secured Web portals, which are increasingly common as organizations move to EMR. But some "secured" Web portals are not actually authorized destinations for confidential data. This Websense solution can monitor SSL traffic and determine if ePHI is being transmitted to a legitimate or unauthorized destination. If the destination is not authorized, the transmission can be blocked, satisfying HIPAA confidentiality requirements. And since no breach has occurred, HITECH Act breach disclosure requirements do not take effect.

Websense Data Endpoint

End-user systems can be used to store and copy ePHI to unauthorized locations. Using endpoint software, Websense® Data Endpoint provides visibility and control as well as discovery of ePHI on end-user systems.

Endpoint visibility and control

The solution can block copy of ePHI to peripheral storage devices by monitoring cut and paste, file access, screen capture, and print jobs for client software applications (including applications with evasive, encrypted network behavior, such as Skype), whether the system is online or offline.

Endpoint discovery and data classification

Laptop theft has been a very common risk area for any regulation governing confidential data, with the potential for thousands of individual records being compromised in a single instance of theft. HIPAA requirements for risk management can be addressed with regular inventory of end-user systems for ePHI and identification of ePHI on these systems. If a laptop is ever stolen, the last detailed discovery job can provide sufficient content to satisfy the breach disclosure requirements of the HITECH Act. More importantly, even before it comes to this, administrators can identify these endpoint systems and require that ePHI be automatically removed from these systems.

Websense Data Discover

Confidential data such as ePHI can be stored on databases, file servers, exchange servers, and Share Point servers as a means for both authorized and unauthorized business use. Websense Data Discover can automatically find and detect ePHI on these systems and take measures to further secure this data as well.

Network discovery and classification

The solution scans the network for various storage systems and identifies ePHI in its various forms — both structured (database) and unstructured data such as files and documents. Detailed reports show all locations and types of ePHI data, allowing administrators to assess their risk profile in the event any of these systems were compromised.

Automated enforcement of stored data

Once ePHI is discovered on stored systems, data owners can be alerted, at which point they can require that specific instances of ePHI be removed or require enhanced access control through updated file permissions. For stored ePHI that is authorized for legitimate use, the business may recommend encryption of this data so that only authorized users can download and view this data. Furthermore, if the data is copied to an external location or an entire disk volume is stolen, the breach is voided since the data is unusable, per the HITECH Act.

Conclusion

Availability of patient records in electronic format continues to grow with modernization efforts across the globe. Visibility and control over ePHI are essential to safeguarding these records against data breaches. Monitoring common business workflows for ePHI and other regulated content helps identify unsecured ePHI and gives data owners a chance to intelligently enforce policy, while enabling legitimate use of email, Web, and client applications.

Blocking unauthorized ePHI disclosure over these applications and securing file permissions on ePHI data stores are recommended to avoid violation of HIPAA confidentiality and integrity requirements. Automated encryption of emails being used for legitimate communication of ePHI also safeguards the data, with zero burden on the end-user. Both blocking unauthorized access and encrypting legitimate access have the benefit of helping to avoid breach disclosure requirements recently mandated by the HITECH Act.

Websense data loss prevention solutions provide visibility and control over common business workflows with a unified policy interface and templates for ePHI policies and reporting to provide operational efficiency. These DLP solutions are essential to successful EMR modernization efforts by helping to safeguard ePHI.

Appendix: Health Care Regulation Mappings

Websense® Data Security Suite provides controls to help entities protect ePHI. The following table highlights regulations impacting the health care industry where the protection of ePHI is explicitly mandated, mapped to Websense DLP solution.

HEALTH CARE REGULATION	WEBSENSE SOLUTIONS AND REGULATION MAPPING
<p>HITECH Act of 2009</p> <p>Breach Notification for Unsecured Protected Health Information:</p> <p>HITECH § 13402 Notification in Case of Breach</p> <p>HITECH § 13404 Application of Privacy Provisions and Penalties to Business Associates of Covered Entities</p> <p>HITECH § 13407 Temporary Breach Notification Requirement for Vendors of Personal Health Records and Other Non-HIPAA Covered Entities</p> <p>45 CFR parts 160 and 164 (Interim Rule) Issued following updates to HIPAA:</p> <p>HIPAA Subpart D—Notification in the Case of Breach of Unsecured Protected Health Information</p> <p>HIPAA §164.404—Notification to Individuals (Description of type of unsecured ePHI involved in the breach)</p>	<p>Breach notification is best served by solutions that proactively inventory where ePHI is stored and when it is in the process of being leaked to an unauthorized location.</p> <p>Websense DLP Solutions provide data leakage prevention for ePHI on the network, endpoints, and data storage systems. Monitoring and preventing data leaks on the network and endpoints combined with routine discovery of ePHI on storage systems helps address ePHI breach notification requirements.</p> <p>Monitoring</p> <ul style="list-style-type: none"> • Monitor end-user systems — on-site, remote, or off-line — where ePHI access is likely for unauthorized copy of ePHI to external devices or local applications with Websense Data Endpoint. • Monitor Web and email traffic for ePHI leaks with Websense Data Monitor. • Routinely discover where all ePHI in the enterprise is stored with Websense Data Discover — to identify which systems need to be secured and also to determine the possible sources of a breach once it has occurred. <p>Prevention</p> <ul style="list-style-type: none"> • Prevent sending of emails to outside entities if they contain ePHI in the message or attachments with Websense Data Monitor. • Prevent uploads of ePHI to unsecured Web locations using Websense Data Monitor. • Prevent end-users — whether on-site, remote, or off-line — from copying or transmitting ePHI to external devices or unauthorized locations with Websense Data Endpoint. <p>Encryption</p> <p>Please see next section on "Safe Harbor" from breach notification requirements.</p>
<p>"Safe Harbor" or Exemption From Breach Notification if ePHI is secured using encryption</p> <p>45 CFR parts 160 and 164 (Interim Rule) (Encryption and destruction for rendering ePHI unusable, unreadable, or undecipherable to unauthorized individuals.)</p>	<p>Websense offers integration with third-party encryption solutions which enable covered entities to protect ePHI and forego breach notification requirements:</p> <ul style="list-style-type: none"> • Enforce automated encryption of email messages and attachments containing unsecured ePHI with integration between Websense Data Protect and third-party encryption solutions. • Enforce automated, policy-based encryption of files and folders with Websense Data Discovery and third-party encryption solutions.

HEALTH CARE REGULATION**WEBSense SOLUTIONS AND REGULATION MAPPING**

45 CFR parts 160 and 164 (Interim Rule) (Keep encryption keys on a separate device from the data that they encrypt or decrypt.)

HIPAA §164.304 Definitions (Encryption)

HIPAA Security Rules

A subset of the HIPAA rules is shown here, covering technical safeguards for ePHI data.

§ 164.306(a)(1) (Protect ePHI: facilities must protect the confidentiality, availability, and integrity of all ePHI created, received, maintained, and transmitted.)

When implemented using the recommended risk assessment and best practices from the NIST “Introductory Guide to Implementing the HIPAA Security Rule” (recommended in the Interim Rule), **WebSense Data Security Solutions** help address confidentiality, availability, and integrity of ePHI.

§ 164.308 (a)(1) Security Management Process (includes required risk analysis and risk management)

IT risk management involves inventory of all assets and related vulnerabilities, threats, the likelihood of these threats, and countermeasures. WebSense enterprise security solutions can help in key areas of the risk management process:

- Discover all enterprise systems that store ePHI data — or assets — with **WebSense Data Discover**.
- Monitor for the threat of data leakage via key infrastructure such as email, Web, and endpoints with **WebSense Data Monitor** and **WebSense Data Endpoint**.
- Establish countermeasures to data leakage by blocking or encrypting data in motion or data in use with **WebSense Data Protect**, **WebSense Data Endpoint**, and routing to **third-party encryption solutions**.

§ 164.308 (a)(5)(i)(Security awareness and training)

§ 164.308 (a)(6) (Implement policies and procedures to address security incidents.)

- Notify users while they are attempting to copy ePHI to unauthorized storage devices or applications using **WebSense Data Endpoint**. Display a pop-up window with the appropriate ePHI protection guidance.

§ 164.308 (a)(5)(ii)(B) (Protection from malicious software (Addressable). Procedures for guarding against, detecting, and reporting malicious software.)

- Monitor and block malicious software from end-user systems, critical servers, emails, and Web transmissions with a combination of **WebSense endpoint, email, and Web security solutions**.

§ 164.308(b)(1) (Business associate will appropriately safeguard information.)

Business associates can implement **WebSense Data Security Solutions** with ease and can leverage policies already in use by the covered entities for which they do business.

HEALTH CARE REGULATION**WEBSense SOLUTIONS AND REGULATION MAPPING**

§ 164.310(d)(1) Device and Media Controls (Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.)

- Maintain a current inventory of ePHI on the network by running discovery scan with **Websense Data Discover**. IT change management can update their data disposal processes to include review of discovery reports so that systems known to store ePHI data can be properly handled.
- Maintain inventory of ePHI on laptops and desktops with discovery scans using **Websense Data Endpoint**. Go further to prevent ePHI copy to external media such as USB storage.

§ 164.312(a)(1) Access Control (Allow access only to those persons or software programs that have been granted access rights.)

- Perform regular discovery of ePHI data on enterprise systems with **Websense Data Discover** to determine where access controls must be in place.

§ 164.312(c)(1) Integrity (Protect electronic protected health information from improper alteration or destruction.)

- Perform regular discovery of ePHI data on enterprise systems with **Websense Data Discover** to determine if data has been modified from previous discovery scan

§ 164.312(e)(1) Transmission Security (Guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.)

- Secure emails between workforce members and external recipients through visibility of ePHI with **Websense Data Protect** and control with **third-party encryption solutions** using "in the cloud" key and encryption service hosting, all with a zero client download.
- **Websense Data Discover**, for stored data on servers and databases

§ 164.514(d) (Collect and use the minimum data necessary.)

Identify duplicate and unsecured copies of ePHI through data discovery:

- **Websense Data Discover**: stored data on file servers and databases, on the network
- **Websense Data Endpoint**: stored data on laptops and desktops, either on the network or offline

Remediate based on this information by requiring data owners or administrators to remove unsecured ePHI.

NIST Guidelines

A few examples of guidelines and questionnaires provided in these publications, to help federal government institutions better secure ePHI data.

NIST Special Publication 800-66: 4.13.Device and Media Controls (§ 164.310(d)(1)) (what data is maintained by the organization and where? Is data on removable media?)

See response to HIPAA Security Rule **§ 164.310(d)(1) Device and Media Controls**

HEALTH CARE REGULATION**WEBSense SOLUTIONS AND REGULATION MAPPING**

NIST Special Publication 800-66: 4.14. Access Control (§164.312(a)(1))(Have all applications/systems with ePHI been identified?, Where is ePHI currently housed?)

See response to HIPAA Security Rule § 164.312(a)(1) **Access Control**

§ NIST Special Publication 800-111: “Guide to Storage Encryption Technologies for End- User Devices” (full-disk encryption, file/folder encryption). This publication is explicitly mentioned in the Interim Rule for the HITECH Act.

Provide both full-disk encryption (for data at rest) and file/folder encryption (for data in use) with routing to **third-party encryption solutions**. Comply with NIST-approved AES encryption algorithm.

Payment Card Industry Data Security Standard (PCI DSS)

Health care institutions routinely accept credit cards as payment for health care services. Retail services on premises such as hospital cafeterias and gift shops also accept credit cards for payment. Any storage or transmission of cardholder data must be protected by the institution.

Twelve categories of controls to protect cardholder data

Multiple solutions within the **Websense DLP Solutions** portfolio. Please see our white paper, “Prevent Leaks and Comply with PCI.”

ⁱIncludes health care providers, health plans (including private and governmental insurance companies), health care clearing house (i.e. processing of non-standard into standard formats by third parties) and most recently, with the HITECH Act, business associates of these entities.

ⁱⁱIncludes health care providers, health care clearinghouse, health plan.

ⁱⁱⁱDepartment of Health and Human Services, “Health Insurance Reform: Security Standards; Final Rule.” *Federal Register*, vol. 68, no. 34 (Feb. 20, 2003), pg. 8341.

^{iv}Department of Health and Human Services, “Health Insurance Reform: Security Standards; Final Rule.” *Federal Register*, vol. 68, no.34 (Feb. 20, 2003), pg. 8358.

^vDepartment of Health and Human Services, Health Information Technology portal: <http://healthit.hhs.gov/>

^{vi}“HIPAA and the HITECH Act: Mark These Important Dates,” *HIPAA Weekly Advisor*, Mar. 23, 2009. (<http://www.hcpro.com/HIM-230135-866/HIPAA-and-the-HITECH-Act-Mark-these-important-dates.html>)

^{vii}Includes health care providers, health plans (including private and governmental insurance companies), health care clearing house (i.e., processing of non-standard into standard formats by third parties) and most recently, with the HITECH Act, business associates of these entities.

^{viii}*ibid.*, pg. 42759.

^{ix}Department of Health and Human Services, “Breach Notification for Unsecured Protected Health Information; Interim Final Rule.” *Federal Register*, vol. 74, no. 162 (Aug. 24, 2009), pg. 42741.

^xBrelsford, James F. “California Raises the Bar on Data Security and Privacy,” Findlaw.com, Sep. 30, 2003. (<http://library.findlaw.com/2003/Sep/30/133060.html>)

^{xi}For more information, refer to the Websense white paper, “Prevent Data Loss and Comply with PCI DSS” (http://www.websense.com/site/docs/whitepapers/en/PCI_ResearchBrief_Web.pdf)