Proactive Compliance:
Find The Right Prescription for Effective Life Science Data Governance

Performance Works
Solving problems that matter

Sponsored by Druva Software Inc. Ltd.

Background

This document summarizes the results of an independent assessment of Druva's product offering targeting Life Sciences. The study's goal was to identify the fit between Druva's inSync data governance and data loss prevention software and the current and emerging market needs of biotechnology, pharmaceutical, and medical device firms. While Druva sponsored this research, Performance Works conducted its assessment independent of Druva using primary and secondary research. It formed its own view of market trends and requirements, and judged the relevance of Druva's inSync to Life Sciences companies based on extensive interviews with IT professionals across the industry.

Life Science Product Development and Information Lifecycle

Introduction

Bringing a drug or medical device to market is complex and costly. Pharmaceutical R&D is a billion-dollar bet. On average, only three in ten drugs marketed become profitable. Beyond competitive, time-to-market pressures, life science IT and compliance professionals must deal with global operations, increased outsourcing of clinical trials and contract manufacturing, accelerating M&A, a growing volume of costly civil and criminal litigation, and a stringent and complicated regulatory environment.

Every stage of the drug and device development cycle is driven by information, the lifeblood of the Life Sciences. The industry must preserve and protect:

- Scientific research
- Clinical trials data and FDA submissions
- Intellectual property (IP)
- Manufacturing quality-assurance assessments
- Marketing communications to physicians, patients, and consumers
- Clinical records received from providers to aid diagnosis and treatment
- Post-market pharmacovigilance reports
- Documents needed for eDiscovery and regulatory investigations

Life Science Information Risks are Increasing

Consumer safety and privacy depend on the quality and integrity of the large volume of information produced by pharmaceutical and device manufacturers. Privacy is complicated by the fact that almost all business information originates in electronic form and must be shared frequently with business associates, who are in turn subject to the same regulations. In the process, critical information is all too easily lost, compromised, or stolen.

Typical information risks include corrupted media, lost or mishandled files, cyber theft, unauthorized disclosure, theft of intellectual property or health records, theft of laptops or other mobile devices, willful destruction of information needed to respond to litigation, and hacking of medical devices to create network vulnerabilities. Any and all of these risks can result in a regulatory data breach (as well as loss of data in a public data breach). And information collected and published by regulatory agencies makes it clear that data breaches are becoming more common. Recent individual data breaches expose data for more patients.

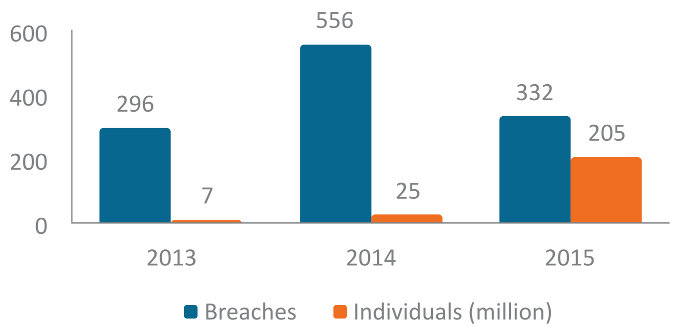

Figure 1: HIPAA Data Breaches and # of Individuals Affected HHS Office for Civil Rights

For the past several years, the life sciences industry has focused particular attention on data breach and related risks defined by the Health Insurance Portability and Accountability Act (HIPAA). HIPAA requires health insurers, healthcare providers, and business associates[1] who store or transmit patient information to follow strict non-disclosure rules so as to protect personal information. In this context, a data breach is the release, without a patient's prior written authorization, of protected Health Information (PHI) including medical records and insurance claims or Personal Identifying Information (PII), such as names, addresses, or social security numbers.

Data breaches that fail to comply with regulations often result in expensive fines, penalties, and potentially litigation. The average corporate data breach (across all industries) costs a firm $6.6M in fines, remediation, lost business, and litigation.[2] For a single breached laptop, fines from the federal department of Health and Human Services (HHS) alone – not counting legal expenses, settlements, or remediation expenses – can be as high as $1.7M.[3]

Among the most severe effects of a data breach is the defection of customers to other suppliers following a publicized legal infraction. Given the publicity surrounding data breaches and other legal actions, Life Science firms have one of the highest rates of annual customer churn (6%) of any industry.[4]

HIPAA Risks Increase: "Another Day, Another HIPAA Breach"

– Healthcare Informatics, 2014[5]

While the absolute volume varies from year to year, the number of individuals affected by HIPAA breaches is increasing annually, and grew many-fold between 2013 and the first seven months of 2015. A shift from theft or loss of physical files to the theft of electronic records magnifies the impact of data loss. Why steal a box of paper records when you can download millions?

"A financial identity can be worth $5 to $10. A medical identity can be worth five to ten times that amount just because of how easy it is to monetize that information once the bad guys get it."

- Robert Clegg, CEO of ID Experts[6]

The public is broadly aware of the risk of credit card theft. However, stolen healthcare records are even more valuable and are a prime criminal target. Compromised or stolen records enable identity theft, misappropriation of healthcare services, fraudulent prescriptions, and insurance and Medicare fraud. Given the many ways in which patient information can be exploited, it comes as no surprise that individual healthcare records are worth as much as $500 on the black market.[7,8]

The kinds of breaches discussed here are not unusual. Hundreds of significant breaches occur annually. According to HHS Office for Civil Rights, nearly 1,300 significant breaches have been reported since late 2009.[9] Individual incidents have compromised the records of millions of patients.[10] Ninety-two million individuals' records were breached between January and May of 2015 alone.[11] At an average cost of $207 per personal record per breach for pharmaceutical companies and $233 for healthcare firms,[12] losses from single incidents can amount to tens or hundreds of millions of dollars in fines, legal expenses, remediation, and settlement costs.[13]

Not only are firms liable for fines after breaches occur, but firms governed by HIPAA (regardless of whether they have suffered breaches) are also subject to HHS Office of Civil Rights audits to identify potential breach risks. One recent audit resulted in a $4.8M fine.[14]

Overall, across all cost factors (fines, remediation, litigation), breaches involving health records cost the industry as much as $5.6B annually.[15]

From the Walled Garden to "Free Range Data"

Current Approach: Protect Information via the Data Center's "Strict" Client Server Model

Performance Works' interviews with life sciences executives indicate that it is common practice for these firms to manage regulated information with a strict, centralized datacenter, client/server IT model. Regulated information is stored on secure servers, subject to rigorous access controls. Less-critical office productivity files are stored on more loosely controlled client-side laptops. Employees in the various scientific and business departments who need access to the regulated content connect to the servers via their laptops or desktop computers and view the files without ever transferring it to their personal systems.

As one senior IT manager from a "Top Five" pharmaceutical company explained during an interview, "What is regulated is not on laptops. What is on laptops is not regulated." Some companies interviewed by Performance Works have gone so far as to equip sales reps with read-only tablet devices to avoid data leakage from this important group of largely mobile workers.

Dealing with the Reality of a Mobile Workforce, Highly Dispersed Information and Cross-Enterprise Data Sharing

"In an ideal world, regulated data would stay on corporate servers, and laptops would store unregulated office work. But we don't live in an ideal world."

-Angela Bazigos, CEO, Touchstone Technologies[16]

Many in the life science and healthcare industries continue to trust the centralized datacenter model to guard against information security risks and data breaches. But IT managers increasingly recognize that information inevitably leaks from protected servers onto workers' mobile devices—often acquired via BYOD––and from there, into the cloud. In 2014, for example, at least 17% of HIPAA data breaches involved hacking or unauthorized access to network servers.[17]

The strict datacenter policies that suggested "regulated data lives on servers," and "productivity data lives on laptops," has eroded. Regardless of what is published in official IT data policy manuals, the reality of data leakage and the risk of major breaches is increasing, as is shown in data from the HHS Office for Civil Rights (OCR). Virtually every HIPAA data breach study has found that laptops are one of the prime causes of HIPAA data breach. In 2013, 35% of breaches were caused by the theft or loss of a laptop or mobile device.[18]

A recent Forrester Research study revealed that 52% of employees accessing patient records store data on their personal computers.[19] Across all industries, 10% of laptops will be lost or stolen during their service life, with most incidents occurring during the first year, particularly during staff travel.[20] Forrester Research estimates that one third of all employees in the health-related industries work outside the office weekly or more. This is a very large population at risk of significant data loss, so the high frequency of laptop-related breach should be no surprise.

Beyond the obvious security risks of device loss or theft, organizations also suffer productivity losses during downtime while an employee waits for IT to provision a replacement device and to restore data. As Performance Works' interviews revealed, many IT managers noted that a single lost device could affect an entire team. This risk applies to people at every level of the organization. Several managers were not shy about noting the impact of careless CEOs mishandling laptops.

Mobility, Data Sharing and the Cloud

IT, compliance, and regulatory affairs professionals must work with other employees to reduce the risks of mobile work and cross-institutional data sharing. Researchers collaborate with colleagues at universities and research labs worldwide. Life science staff share data with business associates and service providers. Scientists contribute clinical trials data to "Big Data" sharing consortia. Life science medical staff share intellectual property (IP) with customers at hospitals and clinics worldwide. Scientists regularly collect data in the field. Nurses at pharmaceutical and device companies advise physicians, observe patients, and collect personal health information, including photographic data, using laptops and cell phones, and they complete sensitive SADRs (Suspected Adverse Drug Reaction reports) on laptops while traveling. Pharmaceutical and device staff must protect clinical information sent to them by providers worldwide in order to consult on the diagnosis and treatment of individual patients. Across these firms, employees travel and share data to support the mission of the organization. By their very nature, mobile work and data sharing put patients and the organization itself at risk.

A practical need for simple, immediate data sharing leads to leakage of regulated data onto laptops, and also to storage of regulated data in cloud applications and repositories. Unfortunately, security studies indicate that many cloud repositories used to store health information are no less risky than the mobile devices that access them. A recent assessment of cloud services used by health professionals found that 77% presented medium risk, 13% were considered high risk and only 9% were "enterprise ready" when evaluated against 54 security criteria.[21]

While managers may find comfort in the safeguards inherent in their current datacenter-centric information governance model, HHS OCR incidence data makes it apparent that the traditional walled garden has been breached.

One leading device manufacturer we interviewed, who is familiar with the older walled-garden approach, instead has adopted a proactive, laptop-oriented data loss prevention program. He has done so because he takes it for granted that sensitive data will reside on mobile devices. After all, he said, "Users are only human." Welcome to the world of Free Range Data.

Core Elements to Mitigating Life Science Information Risks

Performance Works' research identified four most-important, risk mitigation scenarios for pharmaceutical and medical device companies, across major risk scenarios:

- Ensuring data protection without compromising staff productivity, even when devices are lost, stolen, or corrupted.

- Ensuring secure data sharing between partners.
- Providing integrated legal hold management for the collection and preservation of immutable custodian data.
- Enabling automated compliance monitoring for tracking and notification of data risks.

Taking these one by one we'll summarize how Druva's data availability and governance solution, inSync, addresses Life Sciences challenges through the implementation of these elements.

Ensuring data protection without compromising staff productivity, even when devices are lost, stolen, or corrupted.

As the trends presented earlier make clear, the theft or loss of mobile devices significantly impact individual and hence team productivity, while increasing the risk of data breach. Scientists, researchers, and executives travel frequently. Sales representatives generally work outside the office; and their performance depends on continuous access to their critical account plans. Ensuring data protection without compromising staff productivity is a key IT requirement. .

Druva's Approach

The core requirement for uninterrupted worker productivity and data protection is a reliable, readily-available backup of employee data that resides on end-user devices (often referred to as "endpoint devices") and in third-party cloud applications such as Microsoft Office 365. To ensure user satisfaction, creating backups must be nearly invisible to the user – neither requiring user effort nor slowing the performance of user devices. Druva's core product, inSync, protects data with successful backups and restores, advanced encryption, and security mechanisms. To ensure no loss of data or business continuity, end users or IT administrators can then rapidly restore files.

Druva's inSync achieves these goals in the following ways:

- **Seamless backup** of globally deduplicated data on mobile devices or in the cloud, persona backup for preservation of personal settings while ensuring immediate access to data from any device, thereby minimizing downtime and maximizing user productivity.
- **Encryption** of data in-store (256-bit AES) and in-flight (256-bit TLS). inSync uses a patented envelope encryption model that ensures no unauthorized party -- not even Druva -- has access to the data.
- **Data Loss Prevention (DLP)** enables remote wipe (auto-delete) of data on mobile devices and ensures data cannot be accessed on a lost or stolen device. While encryption is necessary, it is not always sufficient. A recent theft at gunpoint forced a physician at Brigham and Women's Hospital in Boston to hand over both the laptop and its password.[22] Remote wipe provides added protection even if hackers or thieves find ways to log onto or hack into lost or stolen devices. inSync's ability to geo-locate or track a device further reduces the risk of unauthorized access of sensitive information.
- **Amazon**-based repository storage, the gold standard in data security and durability, with in-country storage options for life science companies required to meet regional data residency requirements..
- **HIPAA Compliance:** It ought to go without saying that any software touching PHI/PII data must meet special HIPAA software security standards. Druva's software is HIPAA Compliant as defined by the HIPAA Security Rule, and it conforms to HIPAA's five Technical Safeguard standards.[23]

Ensuring Secure Data Sharing Between Partners

Medical staff at life science companies frequently consult with peers at partner and customer sites who use their products to provide care. Whether the task is determining a drug's dosage, fitting implants, or interpreting the results of diagnostic devices, patient care requires the sharing of individual medical records outside the institution's firewall.

Given the need for data sharing across business associates and customers, improper transmission, email or theft of data "in motion" is a common cause of PHI breach, and unintended human error can have costly consequences.[24] Device manufacturer Siemens Medical, for example, attempted to ship seven unencrypted CDs to a business associate, Lincoln Medical and Mental Health Center. The loss of these CDs comprised the claims and diagnostic data and personal identifiers of 130,000 patients.[25]

In addition to regulated PHI data, device manufacturers often share intellectual property over the Internet with customers in the form of software updates and patches. Because these devices are often regulated, so are software changes. The interception or theft of these files not only risks the loss of valuable IP, but can also violate the safety and effectiveness of the device itself. The FBI recently warned that the medical device industry is an active target for hacking and electronic intellectual property theft.[26] Theft of IP increases the risk of device tampering and device infection by bots or malware designed to sabotage devices or to gain access to PHI and internal health networks.

Druva's Approach

inSync provides a secure and complete file sharing repository for the transfer or sharing of IP, PHI, and other sensitive data. Traditional approaches using physical media, email, Internet file transfer protocol (FTP), or popular cloud information sharing repositories all present serious risks. In contrast, Druva's secure PHI data sharing among business associates employs these best-practice technologies:

- **Secure** file transfer with password, expiry, download limits, and tracking.
- **Collaboration** with peer-to-peer and external sharing including permissions control and Active Directory (AD)-mapped sharing groups.
- **Encryption** of the file transfer including data at rest and data in transit ensures HIPAA-compliant exchange of clinical data.
- **Policy-based management**, capable of preventing inappropriate downloading based on content, location, user role, or behavior.

Providing integrated legal hold management for the collection and preservation of immutable custodian data

The life science industry is subject to frequent litigation across a broad spectrum of matters, including securities class action lawsuits, IP and patent litigation, HIPAA violations, FDA sales and marketing regulatory violations, and product liability litigation. These are in addition to the labor, employment, and contract disputes common to any corporation.

The number of civil and criminal investigations against pharmaceutical companies is increasing, and the size of settlements is growing. Individual judgments often amount to hundreds of millions or billions of dollars. 2014 was a particularly active year for FDA and Department of Justice (DoJ) civil and criminal claims against pharmaceutical and medical device manufacturers.

Pharmaceutical-specific laws triggering FDA or DoJ action in 2014 included:

- **The False Claims Act (FCA)** for false or misleading advertising, kickbacks, off-label promotion, and improper billing
- **The Food Drug and Cosmetic Act (FDCA)** for product adulteration
- **Foreign Corrupt Practices Act (FCPA)** governing cases of overseas corruption by U.S. corporations

In 2014, the Department of Justice collected a record $5.6 billion in fines from FCA cases alone, and 500 new FCA cases were initiated, the second highest year for new FCA actions in history.[27]

In any litigation, protecting company information and managing the eDiscovery process is critical. eDiscovery is made more difficult when critical information resides not on central servers but on laptops, mobile devices, and cloud repositories. A quarter of litigation requires placing holds on mobile devices. Failure to do so in a timely manner can itself result in heavy fines. Pharmaceutical company Boehringer Ingelheim, one of the world's 20 largest, was recently fined nearly $1M, in large part for failure to execute a legal hold on employee cell phones in a class action product liability suit. "The duty to preserve is not a passive obligation," the judge said, "It must be discharged actively."[28]

Druva's Approach

Implementing legal hold effectively and efficiently on endpoint devices and cloud repositories uses these approaches and technologies:

- **Built-in legal hold workflow** facilitates the collection of relevant custodian data, suspension of retention policies, and preservation of content in place. The data remains securely stored and immutable and can be easily ingested securely into any eDiscovery platform to begin the legal process.
- **Federated full-text** search enables administrators to locate any file across all users, devices, and storage locations for compliance and legal needs.
- **Tamper-proof audit trails** provide a chronological view of data activities by users and administrators.
- **Fingerprinting** data for authenticity is built in. This collection of extended metadata is done as outlined by the Department of Justice, including documented chain of custody reports for legal admissibility of information and to ensure data is not altered or deleted.
- **Secure file system** access enables ingestion into an eDiscovery platform directly from the inSync repository for further review by legal teams.

Enabling automated compliance monitoring for the tracking and notification of data risks

Minimizing compliance risk is a broad organizational mandate. It includes Sarbanes-Oxley (SOX) regulations on the integrity of financial information and FDA rules regarding clinical trials and the regulation of pharmaceutical marketing. In addition, the newest and most intensely discussed area of risk for IT and Compliance professionals is HIPAA, as defined and revised by its three primary rules:

- **HIPAA Security Rule** (45 CFR 164.306) safeguards the integrity and availability of all electronic PHI (ePHI) data maintained or transmitted on electronic devices. HIPAA mandates the protection of ePHI against threats, hazards, or impermissible disclosure. It also sets security standards for software developers.
- **HIPAA Privacy Rule** (45 CFR 160 & 164 Parts A and E) requires privacy protection for PHI and sets strict conditions for when disclosure is permitted without patient authorization. It identifies the entities covered by HIPAA, including health plans, health providers, and clearinghouses as well as business associates who provide services to those other entities. Pharmaceutical companies and device manufacturers involved in the treatment of patients, including advising physicians, are considered health providers and are, therefore, "covered" by HIPAA. Under certain conditions, other device manufacturers who are not classified as health care providers are considered Business Associates, also covered by HIPAA.
- **HIPAA Breach Notification Rule** (45 CFR 164.400-414) requires covered entities and their business associates to notify the HHS Office for Civil Rights (OCR) of any breach of unsecured PHI.

Given the financial, litigation, and reputation risks involved in PHI data breaches, HIPAA compliance is a top priority for IT, legal, compliance, and regulatory affairs professionals.

As noted earlier, a key challenge for Pharma, Biotech, and Medical Device firms is to ensure information integrity and HIPAA compliance, while reducing the impact of data governance on staff productivity. The variety of locations where data can reside – from laptops and other endpoints to the Cloud – increases pressure on management and makes compliance harder for IT staff and employees alike. Revised 2009 and 2013 HIPAA regulations specify an ever-more-complex regulatory regime.[29] HIPAA's newly issued Omnibus Rule, for example, 563 pages in length, will require the industry to spend 33 million hours annually in compliance related activity, according to HHS' own estimates.[30]

Druva's Approach

While traditional compliance management vendors deal with incidents after they happen, Druva's approach is proactive. inSync monitors and detects risks before they turn into regulatory, civil, or criminal violations, enabling rapid intervention before a risk of data leakage turns into a costly data breach.

In July 2015, a former district sales manager of pharmaceutical company Warner Chilcott, pleaded guilty to submitting fraudulent insurance claims. To commit this crime, he had to commit another: He illegally accessed patient PHI data to create the false claim submissions.[31] Druva's inSync detects these kinds of violations via its predefined templates based on data type (PHI) and automatic detection of data access by an unauthorized staff role (sales).

inSync's Proactive Compliance data governance system provides a company-wide dashboard highlighting all data risks and violations of data governance policies. Druva monitors all employee data sources and looks for potential violations based on monitoring:

- **Content and data sources**, such as PHI, PII or IP data or data identified via full text search or data type, such as social security or credit card numbers
- **User access patterns**, including who is viewing, downloading or transmitting data
- **Location**, including regulated and unregulated endpoint devices and cloud repositories
- **Regulatory categories** or types of risk such as HIPAA violations

This proactive monitoring enables Druva to provide sophisticated, policy-based tracking at a granular level of control. Administrators can leverage predefined templates (or create/customize templates) to monitor specific types of risk, allowing, for example, different jurisdictions to flag different data privacy violations due to differing local regulations. inSync is bundled with pre-defined templates for monitoring data risks unique to life science firms, including HIPAA-covered content, PHI, and PII data, and content covered under other U.S. and state confidentiality laws.

Proactive Compliance: a Closer Look at Druva's Data Governance for Life Science Companies

Whether protecting against data breaches, ensuring compliance with government regulations, responding effectively to legal holds or sharing data with partners, organizations can chose to play offense – anticipating problems before they occur – or play defense, responding only after serious breaches, IP theft, or other losses have happened.

Druva recently extended its widely-deployed inSync platform to focus on playing offense. Druva's philosophy is that information risk is reduced when organizations adopt a proactive data governance strategy. As the judge in the Boehringer case said, data protection isn't a passive obligation; "It must be discharged actively."

Druva developed HIPAA-compliant software to mitigate the kinds of information risks identified in this paper while reducing the data governance burden on IT professionals and on the organization's workforce. Druva's inSync allows Pharma and Biotech firms and Medical Device manufacturers to regain control of regulated and sensitive data in a world of mobile workers, global operations, and data dispersed across mobile devices and the cloud.

The key elements of Druva's Proactive Compliance approach are:

- **Locate** all critical data, whether on laptops, cell phones, or cloud –based applications.
- **Index and protect** all data comprehensively, identifying data types, including regulated or otherwise restricted data based on its inherent content.
- **Monitor** the location, use, access, and movement of all endpoint and cloud data.
- **Alert**, via an organization-wide dashboard, when data use, location, or access is at risk of violating or has violated company data governance policy before they become compliance breaches.
- **Analyze risks** by using powerful full-text search tools and analytics to systematically improve overall data governance.

The tightly-managed datacenter in which all protected data is viewed by endpoint devices, but cannot be downloaded could be seen as the "golden age" in IT control of critical information assets. However, Performance Works' interviews with IT staff at leading life science companies indicated, as supported by our analysis of actual HHS/OCR breach data, this model of control no longer reflects reality "on the ground." Widespread worker mobility, the near-universal adoption of loosely protected laptops and other personal devices, BYOD, and the popularity of cloud applications and repositories (many of them weakly controlled or regulated) present new challenges to IT organizations responsible for managing high-value information and for limiting information risk.

Our research establishes that, given the reality of ever more broadly dispersed data across endpoint devices and the Cloud, a new, active approach to data governance is required to mitigate life science data risks. Druva's Proactive Compliance deals directly with the industry's vulnerabilities and its need for active governance.

Druva inSync's deep indexes of organization-wide endpoint data create a core enterprise information asset that enables easy and automated enforcement of data governance policies. Rather than scramble to react after a breach or loss has occurred, Druva's Proactive Compliance, being an active system, turns an organization's IT and data policy manuals into always-on governance.

Conclusion

Performance Works' interviews with life science IT professionals indicated that data governance is growing in importance. The spread of essentially uncontrolled "free range data" and attendant data risks can only increase the priority of data governance. By making data governance easy to implement, data risk easy to assess, and proactive compliance transparent to deploy, Druva has taken critical steps to allow life science organizations to extend governance to all devices and repositories, especially those well beyond the datacenter. We have little doubt that Proactive Compliance will soon find a place on many life science organizations' short-list of must-have technologies.

About Performance Works

Performance Works solves problems that matter. We analyze markets to help technology companies understand the most critical needs of those they serve while helping users of technology distinguish effective solutions from empty promises. We believe in-depth conversations with decision makers and users are the most-direct path to useful insight. So our process is rooted in primary research and we are grateful to the many professionals who share with us their experience, vision, and frustration in order to help our clients deliver better, more-effective tools and solutions. To direct discussions, we add other types of market analysis to build clarity on what matters to those in the markets we work to understand. Our mission is to help technology companies deliver ever-greater value and, in doing so, improve the lives of those who help us to explore their worlds and interpret their desires.

About Druva

Druva is the leader in data protection and governance at the edge, bringing visibility and control to business information in the increasingly mobile and distributed enterprise. Built for public and private clouds, Druva's award-winning inSync and Phoenix solutions prevent data loss and address governance, compliance, and eDiscovery needs on laptops, smart devices and remote servers. As the industry's fastest growing edge data protection provider, Druva is trusted by over 3,000 global organizations on over 3 million devices. Learn more at ***www.druva.com*** *and join the conversation at* ***twitter.com/druvainc****.*

[1] Business associates include third-party administrators, billing analysis and system vendors, IT and software vendors, benefits management firms, certain types of device vendors–any person or organization that handles or transmits protected health data.

[2] This is an average across all industries, from the most expensive (Healthcare and Life Sciences) to the least expensive (Retail). Retail has a cost per record breach a fraction of that of a Life Science breach. Ponemon Institute, 2009.

[3] *Fierce Health IT*, April 23, 2014. Concentra Health Services, a Humana subsidiary, was fined $1.725M as a result of the theft of an unencrypted laptop.

[4] Ponemon Institute, 2009.

[5] "The Explosion in PHI Data Breaches: Houston, We Have a Problem," *Healthcare Informatics*, April 30, 2014

[6] Report on Patient Privacy and Data Security, Ponemon Institute, March, 2014

[7] Redspin Breach Report, 2014

[8] "Stolen and Lost Devices are Putting Personal Healthcare Information at Risk, Forrester Research, September, 2014

[9] HHS maintains a public portal for all breaches affecting 500 patients or more. See https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

[10] Health Care Informatics, July 31, 2014

[11] *HIPAA Journal,* June, 2015.

[12] Ponemon Institute, 2013

[13] Anthem's 80 million record breach could cost the firm as much as $1B, even though PII records rather than patient health records were compromised.

[14] "Data Breach Results in $4.8 Million HIPAA Settlements," US Department of Health & Human Services (http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/jointbreach-agreement.html).

[15] Experian 2015 Data Breach Forecast.

[16] Interview with Angela Bazigos, is CEO of Touchstone Technologies, a firm that advises the FDA and major pharmaceutical and device manufacturers on data and IT compliance issues. She is co-author of *Computerized Systems In Clinical Research: Current Data Quality and Data Integrity Concepts,* Drug Information Association, 2011.

[17] US Department of Health and Human Services, Office for Civil Rights, *HIPAA Breach Portal:* https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf, Performance Works' analysis of breach data for 2014, in which at least 96 of 556 breaches involved hacking or unauthorized access or intrusion on network servers.

[18] US Department of Health and Human Services, Office for Civil Rights, *HIPAA Breach Portal:* https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf, Performance Works' analysis of breach data for 2013.

[19] "Stolen and Lost Devices are Putting Personal Healthcare Information at Risk," Forrester Research, September 2014. See also: "Security Risks Faced by Healthcare Providers Empowering Mobile Moments to Clinical Teams," Forrester Research, December 2014.

[20] "The Billion Dollar Laptop Study," Intel Corporation and Ponemon Institute, 2010

[21] "Risks and Cyber threats to the Healthcare Industry," *INFOSEC Institute*, September 16, 2014.

[22] *Health IT Security,* November 2014.

[23] HIPAA software compliance is outlined in HIPAA's Security Checklist, http://www.ihs.gov/hipaa/documents/IHS_HIPAA_Security_Checklist.pdf

[24] Experian's *2015 Data Breach Report* found that, "The majority of data breaches originate within the company walls. Employees and negligence are the leading cause of security incident…."

[25] US Department of Health and Human Services, Office for Civil Rights, *HIPAA Breach Portal:* https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

[26] "Risks and Cyber threats to the Healthcare Industry," *INFOSEC Institute,* September 16 2014.

[27] "2014 Year-End FDA and Health Care Compliance and Enforcement Update: Drugs and Devices," Gibson Dunn, January 14, 2015.

[28] Southern District Court of Illinois, In Re Pradaxa, Case 3:12-md-02385-DRH-SCW, Document 320, Filed 12.09.13. http://www.aceds.org/wp-content/uploads/2014/01/In-Re-Pradaxa-12-9-13-Opinion-.pdf

[29] For details about HIPAA PHI compliance, see Druva's white paper, *Endpoint Backup Compliance Considerations for HIPAA-regulated Enterprises,* http://pages2.druva.com/HIPAA-Backup-Compliance-whitepaper-web.html

[30] "HITECH HIPAA Restrictions on Refill Reminders and Patient Communications," *Policy and Medicine,* November 5, 2013.

[31] US FDA, Criminal Investigations website: http://www.fda.gov/iceci/criminalinvestigations/ucm453875.htm

Q216-CON-10528