KeepItSafe®
ONLINE BACKUP

HOW TO HANDLE THE DATA COMPLIANCE

CHALLENGES FACING **YOUR IT TEAM** AND YOUR BUSINESS

www.keepitsafe.com

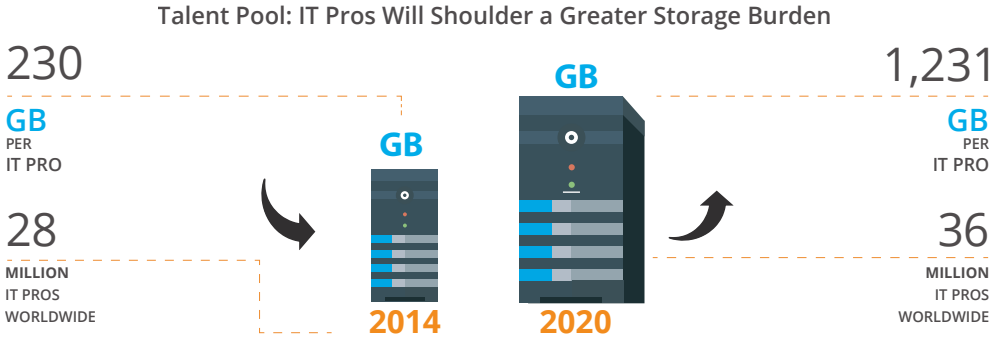
TABLE OF CONTENTS

INTRODUCTION

If you are responsible for the IT infrastructure of a business in today's digital era, you are facing some significant challenges.

First, the sheer volume of data you're charged with managing, securing and archiving is likely massive and growing rapidly — doubling every couple of years, according to IDC Research.[1] And although 75% of data is generated by individuals, businesses will have some responsibility for protecting at least 80% that data at some point.[2]

A related challenge is the rapidly rising number of platforms and devices on which your business data is being stored and transmitted. A Juniper Networks survey found 40% of employees use personal mobile devices to access company data.[3] Also, the Ponemon Institute found 35% of business data is stored in the cloud — and almost half of this data is not controlled by the company's IT department.[4]



IDC Research: The Digital Universe and Big Data [5]

Moreover, because your corporate data is increasingly valuable to hackers, you also have to contend a growing threat of cyberattacks. Indeed, 2015 was one of the worst years on record for corporate data breaches. As Forbes reported, hackers stole or compromised more than 100 million personal records that year from healthcare organizations alone.[6]

But in addition to all of these challenges — maintaining responsibility for an exponentially increasing volume of corporate data, keeping track of this data across an ever-expanding list of devices and cloud apps, and protecting your network from cybercriminals — you have yet another issue to worry about: **federal regulators.**

This paper will discuss the complexities of some of the major federal regulations governing data privacy, offer suggestions for complying with them, and give you guidance on what to look for in a partner for one critical aspect of data compliance — an offsite backup and recovery solution.

DATA PRIVACY REGULATIONS APPLY TO MORE BUSINESSE THAN YOU MIGHT

THINK MAYBE EVEN YOURS

If you have only limited familiarity with the major data privacy regulations, you might assume they apply only to a few very specific types of high-profile businesses. HIPAA, for example, governs the healthcare industry. Sarbanes-Oxley applies only to publicly traded companies (and all of their wholly-owned subsidiaries).

For the most part, these assumptions are correct — but for only some of the key regulations. For others, the regulatory net is cast wider than you might realize, and some of these regulations likely apply to your business as well.

To cite one example, the Gramm-Leach-Bliley Act (GLBA) — a 1999 law dealing primarily with the powers of banking organizations — includes a data privacy rule that requires financial institutions to adopt policies and procedures to safeguard customer records and information.

But this law defines "financial institution" extremely broadly, to include any organization that engages in financial activities as part of its normal business operations. This means that many other types of companies, which wouldn't identify themselves as financial institutions, are subject to the rules of GLBA — businesses such as real estate brokerages, insurance agencies, investment advisors and collection agencies. Even retailers might fall under GLBA's regulations, if they offer their own credit cards to customers.[7]

What this means for your business is that, if part of your normal operations includes handling, storing or transmitting customers' personally identifiable information (financial data, medical history, etc.), then your company might fall under one or more of the major federal privacy regulations.

Let's take a brief look at some of these regulations, and what their requirements mean in terms of your IT team's responsibility to ensure your company complies with them.

SNAPSHOT OF DATA PRIVACY REGULATIONS

REGULATION	WHAT THE REGULATION REQUIRES	HOW IT TEAMS CAN COMPLY
HIPAA (Health Insurance Portability and Accountability Act)	HIPAA seeks to establish standardized mechanisms to ensure healthcare organizations (called "Covered Entities") protect the integrity, privacy and confidentiality of individuals" health-related data	**1.** Make data backups **2.** Establish access controls based on job responsibility **3.** Log successful access attempts to mission- critical resources **4.** Limit unsuccessful user ID login attempts after consecutive unsuccessful tries **5.** Require authentication **6.** Enable system events (logging) **7.** Encrypt information **8.** Keep data physically and electronically secure from unauthorized access (implement security tools to prevent malicious attacks or detect intrusions, restrict Internet access to DMZ)
FDA (Food & Drug Administration) Part 11	Part 11 requires drug makers, medical device manufacturers, biotech companies, and other FDA-regulated industries to implement controls, including audits, system validations, audit trails, electronic signatures, and documentation for software and systems involved in processing electronic data.	
GLBA (The Gramm-Leach-Bliley Act)	GLBA, also called the Financial Modernization Act of 1999, includes provisions to protect consumers' personal financial information held by companies broadly defined as "financial institutions."	
SOX (Sarbanes-Oxley Act) Section 302	SOX is designed to protect investors by improving the accuracy and reliability of corporate disclosures. Section 302 requires certification of financial statements by both the CEO and the CFO. IT departments supporting financial institutions will also have to ensure the accuracy of these records.	**1.** Establish access controls based on job responsibility **2.** Log successful access attempts to mission- critical resources **3.** Require authentication **4.** Enable system events (logging) **5.** Keep data physically and electronically secure from unauthorized access **6.** Data retention: 7 years' retention for audit reports and related materials **7.** Immutability: Prevent the alteration, destruction, concealment, falsification, of any record or document

REGULATION	WHAT THE REGULATION REQUIRES	HOW IT TEAMS CAN COMPLY
EUDPD (EU Data Protection Directive)	The EUDPD declares that data protection is a fundamental human right. It standardizes protection of data privacy for EU citizens.	**1.** Make data backups **2.** Establish access controls based on job responsibility **3.** Require authentication **4.** Enable system events (logging) **5.** Encrypt personal information
Basel II Capital Accord	This rule requires banks to put in place Business Continuity and Disaster Recovery plans to ensure continuous operation and to limit losses.	**1.** Make data backups **2.** Archiving, retrieval and restoration capabilities should be in place **3.** Data retention of 3–7 years of data history
PIPEDA (Canada's Personal Information Protection & Electronic Data Act)	This law requires organizations to obtain consent when they collect, use or disclose personal information. It also declares that businesses should supply an individual with a service or product even if they refuse consent for the collection or use of their personal data, unless that data is essential to the transaction. It also demands personal information policies be clear, understandable and readily available.	**1.** Make data backups **2.** Establish access controls based **3.** On job responsibility **4.** Require authentication **5.** Enable system events (logging) **6.** Encrypt personal information
HITECH (Health Information Technology for Economic and Clinical Health Act)	The HITECH Act broadens the scope and increases the rigor of HIPAA compliance. For protecting of Protected Health Information (PHI) data, these key areas are especially important: • Expansion of HIPAA rules to business associates • Stricter requirements for breach notifications • Encryption as a recognized methodology or protecting PHI	**1.** Encrypt data **2.** Destroy data when appropriate

REGULATION	WHAT THE REGULATION REQUIRES	HOW IT TEAMS CAN COMPLY
FISMA (Federal Information Security Management Act)	The FISMA law defines a comprehensive framework to protect government information, operations and assets against natural or manmade threats.	The National Institute of Standards and Technology (NIST) outlines nine steps toward compliance with FISMA: **1.** Categorize the information to be protected **2.** Select minimum baseline controls **3.** Refine controls using a risk assessment procedure **4.** Document the controls in the system security plan **5.** Implement security controls in appropriate information systems **6.** Assess the effectiveness of the security controls once they have been implemented **7.** Determine agency-level risk to the mission or business case **8.** Authorize the information system for processing **9.** Monitor the security controls on a continuous basis
FINRA (Financial Industry Regulatory Authority)	Formed by consolidating redundant rules under NASD (Rule 3510) and NYSE (Rule 446), FINRA member companies must maintain business continuity and contingency plans to satisfy obligations to clients in the event of an emergency or outage. It requires members to create, test, and update business continuity plans to satisfy obligations to clients in the event of an emergency or outage.	**1.** Develop and deploy a Business Continuity Plan **2.** Develop and deploy a Disaster Recovery plan
SEC (Securities and Exchange Commission) Rules 17-a 3 and 4	These rules require broker-dealers to create, and preserve in an easily accessible manner, a comprehensive record of securities transactions they effect and of their business in general. Rule 17a-4 requires electronic storage to preserve records in a non-rewriteable and non-erasable format. Retention is required for a specific period of time.	**1.** Make data backups **2.** Encrypt data **3.** Retain data for required period

REGULATION	WHAT THE REGULATION REQUIRES	HOW IT TEAMS CAN COMPLY
FERPA (The Family Educational Rights and Privacy Act)	This law is designed to protect the privacy of student education records and applies to all schools that receive funds under programs of the US Department of Educations.	**1.** Make data backups **2.** Establish access controls based on job responsibility **3.** Log successful access attempts to mission- critical resources **4.** Limit unsuccessful user ID login attempts after consecutive unsuccessful tries **5.** Require authentication **6.** Enable system events (logging) **7.** Encrypt information **8.** Keep data physically and electronically secure from unauthorized access (implement security tools to prevent malicious attacks or detect intrusions, restrict Internet access to DMZ)

DATA PRIVACY REGULATIONS ARE VAGUE AND CONFUSING

Even from reading only the above short overviews of these data privacy laws, you can likely discern that the laws themselves do not offer step-by-step instructions for compliance. Instead, the laws use phrases such as "reasonable" and "appropriate" to describe the measures businesses must take to ensure the integrity and confidentiality of the sensitive data they handle.

Indeed, because these regulations deal with the security of digital files and records, the lawmakers were intentionally non-specific in crafting the language to allow businesses and IT departments to implement the measures that reflected the most advanced technology and best practices available at the time.

Of course, this presents a challenge to you as an IT professional responsible for meeting your company's data compliance requirements: Even if you develop and deploy solutions and processes to safeguard your customers' personal data, you still cannot know for sure that those processes will hold up under a regulatory audit.

Here are just a few of many examples of where the most critical components of these data privacy laws are written to be non-specific and open to interpretation:

GLBA (GRAMM-LEACH-BLILEY ACT)
TITLE 5; Section 501(b): Financial Institutions Safeguards

> *"Each agency or authority described in section 501(a) **shall establish appropriate safeguards** for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards... 1) to insure the security and confidentiality of customer records and information; 2) to **protect against any anticipated threats or hazards** to the security or integrity of such records; and 3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer."* [8]

What, precisely, does the law mean by "appropriate safeguards" here? The language doesn't specify. Nor does it clearly state what is meant by protecting against "anticipated threats or hazards," or if a company regulated under GLBA would be in compliance if it suffered a non-anticipated threat.

HIPAA (HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT)
SUBTITLE F; Section 262: Administrative Simplification

> *"Each person described in Section 1172(a) who maintains or transmits health information **shall maintain reasonable and appropriate** administrative, technical and physical safeguards...."* [9]

HIPAA, too, leaves much of its most important rules open to interpretation — such that different companies, both trying in good faith to comply with its provisions, will almost certainly develop and deploy very different solutions for satisfying these requirements.

Also worth noting: Although it is widely understood by experts on data privacy regulations that a key component of compliance is encrypting your data, nowhere in HIPAA's thousands of words of main text will you find the word "encrypt." This all-important step is another in a long list of data protection methods that HIPAA's lawmakers leave to the discretion of the IT departments at each "Covered Entity."

And don't forget: These are not industry standards or association guidelines; they are government regulations backed by the full force of federal law. So you need to be as confident as possible — knowing you can never be 100% certain — that your company's processes will withstand your regulators' scrutiny.

TOP COMPLIANCE PROBLEMS FACING IT DEPARTMENTS TODAY

Clearly, developing a comprehensive plan to ensure your business stays on the right side of whichever data privacy regulations govern your industry is a complex undertaking.

To give you an idea of where many other businesses have made compliance missteps, here is a brief list of organizations' biggest compliance challenges, compiled by CIO Magazine[10] based on interviews with many technology professionals and compliance experts:

EMPLOYEE ERROR

Even if an IT department puts in place firewalls, intrusion detection and prevention systems, and other security measures to safeguard its networks, the company can still find itself out of regulatory compliance if its employees innocently mishandle the company's regulated data.

Examples include employees leaving personal customer or patient data on unsecured computers or printed out on hardcopies that can be viewed or grabbed by personnel not authorized to view that data. They could also include employees falling for phishing or other hacker ruses to illegally obtain access to regulated data.

Recommendation:
The key measure here is proper training of your staff. Every employee who handles or has access to company data that falls under federal regulation needs to know how to protect that data.

LOST, STOLEN OR HACKED LAPTOPS

One of the main culprits of noncompliance with data privacy regulations is the use — or, more accurately, the misuse — of company laptops.

To cite two examples of major recent laptop-related HIPAA violations, the Department of Health and Human Services announced in 2014 that two businesses, Concentra Health Services and QCA Health Plan, agreed to pay fines totaling nearly $2 million. Both HIPAA violations were the result of these health organizations failing to physically secure and digitally encrypt laptops containing electronic protected health information of their patients. [11]

Recommendation:
A key safety measure here as well is proper employee training. Employees carrying laptops anywhere need to keep those machines password-protected, physically under their care at all times and away from public WiFi hotspots, such as coffee houses, whenever possible.

Another security measure that experts suggest is to issue employees travel-only laptops — which are capable of performing the employees' specific job tasks but limit access to the company's network and do not store regulated data.

LACK OF CONTROL OVER MOBILE DEVICES

IT departments face an ever-growing challenge of protecting their company's network and data as more and more mobile devices enter their facilities (both company-issued and personal devices) and access their corporate data.

Even if an IT team secures all of the machines in its facilities that contain (or can be used to access) regulated data, what happens when an employee enters the office and uses a personal smartphone or tablet to access this data or to share it with vendors or other third parties outside the firewall?

Recommendation:

Protecting corporate data on mobile devices will require a comprehensive mobile data management solution — including remote-wipe capability.(This can also be invaluable to install onto your staff's laptops, in the event that an employee loses a machine on the road, for example.)

An effective mobile device management solution will also allow your team to configure devices such that they can download or access only authorized apps.

THE USE OF THIRD-PARTY APPS NOT UNDER IT'S CONTROL

The use of apps not authorized or controlled by the company — for example, remote employees collaborating using Dropbox or Google Drive — is often cited as one of the primary compliance challenges.

Because employees often find it faster and easier to do their work with unsanctioned tools or services, the company is often by definition out of compliance with its data privacy regulations — because a key component for compliance is that the company maintain official oversight of regulated data wherever it resides or travels.

Recommendation:

The experts here generally recommend two measures be taken in parallel. First, the company needs to educate its employees such that they understand going outside the organization's officially approved tools for data storage or collaboration exposes the business to a compliance violation.

Second, the experts suggest the company more quickly assess and adopt services that its employees need to perform their work.

THE USE OF CLOUD SERVICE PROVIDERS WHO DON'T MEET COMPLIANCE STANDARDS

Another major compliance challenge, one that often goes completely undetected until it's too late, is that businesses often entrust their regulated data to cloud providers — for storage, backup, collaboration or transmission — and the measures those providers take with the businesses' data fall short of compliance.

For example, cloud security firm SkyHighNetworks reports that fewer than 10% of all cloud vendors encrypt their customers' data while it's at rest in the vendor's cloud storage. [12]

But there are many other ways that cloud service providers can undermine your compliance efforts — such as not maintaining your data on secure servers, not taking physical and administrative precautions to protect your data all times in their data centers, and keeping your data in only a single location.

As you might recall from the language of several of the data privacy regulations we've discussed, compliance requires the data be easily accessible and protected against anticipated threats and hazards; these could include natural disasters or outages that could compromise the data stored in any one data facility.

Recommendation:
Before committing your company's regulated data (or even your non-regulated data, for that matter) to a cloud service provider, you will need to conduct a thorough vetting of that company's regulatory compliance practices.

Even a superficial investigation while you're researching potential cloud partners — such as asking them if they know about the data regulations governing your industry — will reveal that the cloud vendor has no idea how to keep your data in compliance.

OUTDATED OR ANACHRONISTIC REGULATIONS

Perhaps the most difficult aspect of complying with your industry's data privacy regulations will be the language of those regulations themselves.

As we've discussed, lawmakers crafted these regulations intentionally to be non-specific and open to interpretation. The idea was that rather than spell out specific machines, encryption protocols or best practices for IT teams to deploy — all of which would eventually become outdated — the law would serve more as a guide as to what regulators expected from businesses to safeguard their customers' data.

Problem is, even in their non-specific forms many of these laws today have become outdated and much more difficult for even the most diligent and conscientious IT departments to follow.

For example, as we stated in the introduction, businesses are generating and gathering exponentially more data today than they were when most of these laws were written, and this data is showing up in an increasing number of devices and cloud services. But several of these data privacy laws require all regulated data to be digitized.

Additionally, some of these regulations — most notably HIPAA — place pressure on regulated businesses to manage the vendors who handle their data. Because most HIPAA-regulated organizations have to deal with an ever-greater number of vendors for their businesses to operate effectively, this presents an increasing challenge.

Recommendation:
It is precisely because these data privacy regulations are becoming more outdated with each passing year that the businesses governed by them need to pay greater attention to their processes — to ensure they are not unintentionally running afoul of their regulators.

For these reasons, the experts — including us — agree that your IT team will need to perform thorough due-diligence on any potential partner, vendor or business associate if that company will in any way handle or have access to the regulated data in your care.

DATA BACKUP, RECOVERY AND ENDPOINT PROTECTION:
HOW TO ENSURE YOUR PROCESS IS COMPLIANT
(AND YOUR VENDORS DON'T UNDERMINE YOUR EFFORTS)

Here we would like to walk you through how to develop — or, far more cost-effectively, to outsource — a comprehensive solution for data backup, disaster recovery and endpoint protection that will not only protect your data but also keep your company on the right side of regulators.

This list will not be exhaustive. There are many variations to these steps, and some of the steps identified here might not apply to you. Moreover, data privacy regulations are written specifically such that there is no way to know when your company is "done" with your compliance process.

What we will provide you here, however, is a set of best practices for regulatory compliance that has been proven year after year, with thousands of customers across many industries, to keep a business compliant with its industry's data privacy regulators.

COMPLIANT DATA BACKUP:

1. Stored offsite, using the most advanced encryption-at-rest protocols available (which, today, is 256-bit AES encryption).
2. Ideally stored in multiple offsite locations — and these different data centers should be in geographically distinct regions, so that the data can still be retrieved quickly even amid a regional disaster or outage.
3. Your data at these offsite facilities should be stored on high-end disk arrays that cannot be changed once they are backed up (inability to rewrite the data once backed up is a key component of compliance with certain regulations, such as SOX).
4. These data facilities should also include physical security (guards, badge- or biometric-restricted access) and should not allow for human tampering.
5. The encryption code should not be sent to your offsite data center's facilities, such that even if they are hacked, the attackers will be unable to access your data.
6. Your offsite data facility should capture and store all backup and restore activity, for audit purposes and for your record-keeping.
7. Your data center should restrict login privileges to only those with admin credentials.
8. The data center should conduct integrity checks on your data at regular intervals that you specify — nightly, for example.
9. You should be able to set up retention rules with your data storage provider, based on either your business's needs or the requirements of your industry's regulations.

10. Your offsite data center should also have the following credentials:

a. ISO-27001 Security Certification
b. SSAE16 Audit Completion
c. FIPS 140-2 Secure Transmission Protocols for Backing Up Your Data to their Location

11. Finally, if you choose to outsource data backup to a cloud provider, you should work only with a "white glove" firm, meaning a company that fully manages and monitors your data at all times and handles any issues proactively on your behalf.

COMPLIANT DATA RECOVERY AND BUSINESS CONTINUITY:

12. Your disaster recovery solution should include a fully documented, step-by-step recovery plan for servers, including precise restore instructions.

13. Your process should include staff training for all processes to ensure clarity of roles and responsibilities during a crisis. If you outsource, your cloud backup and recovery vendor should offer this training to your organization.

14. Your process must include testing and exercises — ideally at least annually — to test recovery, restore and failover capability for your mission-critical data.

15. If you are regulated by HIPAA and choose to outsource these backup and recovery functions to a cloud provider, you should also insist that the company sign a Business Associate Agreement; this will enable you to share responsibility for data protection compliance with this vendor.

COMPLIANT ENDPOINT PROTECTION AND MOBILE DEVICE MANAGEMENT:

16. Your solution will need to support your organization's entire digital footprint — including smartphones, laptops, tablets, etc.

17. Ideally, your in-house compliance teams (or your cloud vendor, if you outsource) will be able to easily search across all of your end-user data to identify data risks — without impacting employee productivity.

18. You will want to deploy a solution that offers a consolidated data dashboard that enables your IT team to manage policies, monitor and assess data risks and review activity history to ensure ongoing compliance.

19. You will want to implement a solution for elastic indexing of regulated data (because your needs will change over time).

20. You will also want a comprehensive Data Loss Prevention (DLP) program for all of your endpoint devices, in which an administrator can geo-locate a lost or stolen device and even remotely wipe its contents to factory settings.

As you can see, implementing all of these measures in-house will be an enormous undertaking. Moreover, without an ongoing relationship with an expert data protection partner, you and your IT team will have the additional burden of keeping up with your industry's data privacy regulations — to ensure you don't fall out of compliance after all of this difficult implementation work.

For these reasons, we recommend you team up with an industry leader in cloud backup and disaster recovery — a business that for many years has been helping business customers around the world not only securely back up their data but also stay on the right side of federal regulators.

INTRODUCING
KEEPITSAFE

For more than a decade, **KeepItSafe** has been a world leader in compliant cloud backup, disaster recovery and endpoint protection — serving more than 20,000 corporate customers, across four continents, and protecting more than 50 petabytes of mission-critical data every year.

We offer a premium, white-glove service for cloud backup, recovery and business continuity — and we are among the only global recover providers awarded ISO 27001 certification for information security management

Visit our website, **www.KeepItSafe.com**, to learn more about our industry-leading solutions for cloud backup, disaster recovery and endpoint protection.

Or contact us anytime to schedule your free Network Evaluation and Data Protection Assessment, as well as to begin a free trial of our solution.

888 965 9988

sales@keepitsafe.com

Sources:

1. **InfoWorld —"How to Survive the Data Explosion"**
   http://www.infoworld.com/article/2608297/infrastructure-storage/how-to-survive-the-data-explosion.html
2. **ComputerWorld—"World's Data Will Grow By 50x in Next Decade"**
   http://www.computerworld.com/article/2509588/data-center/world-s-data-will-grow-by-50x-in-next-decade--idc-study-predicts.html
3. **TechTarget — "Top 5 Mobile Data Protection Best Practices"**
   http://searchsecurity.techtarget.com/tip/Top-5-mobile-data-protection-best-practices
4. **Ponemon Institute and Gemalto "2016 Global Cloud Data Security Study"**
   http://www2.gemalto.com/cloud-security-research/
5. **IDC Research — "The Digital Universe and Big Data" study**
   http://www.emc.com/leadership/digital-universe/2014iview/business-imperatives.htm
6. **Forbes — "Data Breaches in Healthcare Totaled Over 112 Million in 2015"**
   http://www.forbes.com/sites/danmunro/2015/12/31/data-breaches-in-healthcare-total-over-112-million-records-in-2015/#63e61a07fd5a
7. **Minnesota State Bench & Bar — "Is Your Practice Subject to Gramm-Leach-Bliley?"**
   http://www2.mnbar.org/benchandbar/2001/sep01/financial-privacy.htm
8. **GLBA Text, Government Printing Office**
   https://www.gpo.gov/fdsys/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf
9. **HIPAA Text, Government Printing Office**
   https://www.gpo.gov/fdsys/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf
10. **CIO Magazine — "7 Biggest Compliance Headaches"**
    http://www.cio.com/article/2382445/compliance/7-biggest-it-compliance-headaches-and-how-cios-can-cure-them.html
11. **HHS Press Release — "Stolen Laptops Lead to Important HIPAA Settlements"**
    http://www.hhs.gov/about/news/2014/04/22/stolen-laptops-lead-to-important-hipaa-settlements.html
12. **SkyHighNetworks — "You Won't Believe the Popular Apps That Don't Encrypt Your Data"**
    https://www.skyhighnetworks.com/cloud-security-blog/only-9-4-of-cloud-providers-are-encrypting-data-at-rest/