**Is HIPAA compliance the reason for data leaks?**
Give a bureaucracy enough time, and they’ll come up with something like HIPAA (Health Information Portability and Accountability Act). It’s a noble effort to secure and protect your health information. But, it creates a compliance challenge that puts its original intent in jeopardy.

Despite scores of pages on compliance with privacy and security mandates, HIPAA still sees repeated data leaks. You might even wonder if HIPAA compliance is the reason for data leaks?

**Compliance with** [**Privacy Rule**](http://www.caringinfo.org/files/public/ad/HIPPA_Privacy_Rule.pdf)

Covered Entities (CE) - healthcare providers, employee group health plans and their insurance carriers, and government healthcare programs - are required to proactively protect the privacy of your health information and records. The Privacy Rule specifies how and with whom your protected health information (PHI) may and may not be shared.

**Compliance with** [**Security Rule**](https://www.nist.gov/healthcare/security/hipaa-security-rule)

Developed by NIST (National Institute of Standards and Technology), the HIPAA Security Rule safeguards electronic protected health information (EPHI). All CEs must protect the “confidentiality, integrity, and availability of EPHI. . . against reasonably anticipated threats, hazards, and impermissible uses and/or disclosures.”

**So, what’s the problem?**

The adoption of digital records and the rise of cybercrime have challenged the practical applicability of the HIPAA rules let alone protecting it from criminal assault. The [cost of non-compliance](https://www.paubox.com/blog/hipaa-compliance) can be very significant.

For example,

* [$1.5 million settlement](http://www.ama-assn.org/ama/pub/physician-resources/solutions-managing-your-practice/coding-billing-insurance/hipaahealth-insurance-portability-accountability-act/hipaa-violations-enforcement.page) against North Memorial Healthcare of Minnesota
* $750,000 settlement agreement with Raleigh Orthopedic Clinic in North Carolina
* $275,000 against one of Prime Healthcare’s 23 hospitals in California
* $2.25 million paid by CVS Caremark pharmacies

Many fines are smaller, and the sizable penalties indicate more egregious violations. Nonetheless, they show the government’s intent to enforce its HIPAA compliance rules.

Moreover, most practitioners lack the tech sophistication to manage the risk presented by HIPAA security guidelines. So, they rely on software or on third-party relationships.

**The forensic analysis**

**Software:** KIVU Labs perform forensic analysis on cyber security, and it finds problems with reputable software for Electronic Health Records (EHR) and Electronic Medical Records (EMR). [In a recent report, KIVU concluded](https://kivulabs.com/hipaa-data-leakage-is-your-protected-health-information-secure/), “While the vendor software itself may meet the requirements of HIPAA compliance for the discrete functions it performs, the truth of the matter is that no software or system that handles Protected Health Information (PHI) is HIPPA compliant until it has undergone a risk assessment by the regulated entity to determine the efficacy of its security controls in the user’s environment.”

**3rd-Party:** [Grant Thorton, Ltd., experts in provider financial reporting, feels](https://www.grantthornton.com/~/media/content-page-files/health-care/pdfs/2013/HC-2013-AIHA-wp-HIPAA-rule-data-control-concerns.ashx), “Increased use of third-party vendors for applications and data processing services is a business model that is likely to continue . . . Unfortunately, many have learned the hard lesson that expected cost efficiencies and other benefits associated with third-party custodians of an organization’s confidential data can quickly be outweighed by data breaches that result in fines, civil penalties and damaged reputations.”

In anticipation of a HIPAA compliance audit, you need to take and document some preventive measures whether you’re dependent on manual records, program software, or third-party relationship:

* **Operational Policy:** CEs have a duty to prepare and communicate policies. They are required to train all staff on their roles and responsibilities. And, they are advised to craft processes and workflows with assigned accountabilities for handling PHI.
* **Control Access:** Leadership must decide on levels of authorization and methods of access. Systems must distinguish the authorized and non-authorized based on pre-determined risk-based privileges.
* **Operating System:** Smartphones, tablets, laptops, and other platforms are used to access, read, expand, and archive records. The software and device operating systems have to integrate, or risk increases. [According to KIVU](https://kivulabs.com/wp-content/uploads/2015/10/HIPAA-Data-Leakage-Paper-Jan-2015ACS-REVISED-OCT-2015.pdf), “Software applications require security reinforcement at the file, directory and server level to protect PII/PHI-containing files stored outside secured database environments.”
* **Classify Data:** Providers must classify the data in question. Some data is more private than other data. Some can be used for certain needs and not others. Various records have degrees of sensitivity, importance, and potential impact, and they need to be tagged as such.
* **Mobile Encryption**: All mobile devices must have access and encryption controls. Policies and protocols must also limit the authorization to use mobile devices to handle HIPAA protected records.
* **Uncompromised Software:** Some users are tempted to “customize” the compliance software to speed performance or differentiate between users and security level. The same independence drives them to delay upgrades and adjust configuration, all of which jeopardize the security.
* **Secure Channels:** Sensitive data sent between data centers must be encrypted to reduce breaches. Any protocol must include integrity controls to make sure that it identifies any modification of the data.
* **Breach Response:** All parties mustunderstand the importance and protocol for informing authorities and patients when a data breach occurs. It’s disaster planning that cannot be avoided despite embarrassment or awkwardness of the admission. But, it’s also smart to confirm the security of the data centers, transmission connections, and software performance record.
* **Conduct audits:** Although it is very time-intensive, keeping logs of regular formal audits of the provider’s security performance will find strengths, vulnerabilities, and failures in its systems. Of course, such audits require evidence of response to risk and mistakes.
* **Outside Assessment:** Things change over time. Those changes include HIPAA regulations, software applications, and criminal threats. CEs are urged to secure periodic third-party forensic assessments.

**So, is HIPAA compliance the reason for data leaks?**

A recent report by the [Health Information Trust Alliance (HITrust) blames](http://www.physicianspractice.com/blog/what%E2%80%99s-leading-cause-hipaa-data-breaches-you-may-be-surprised) most breaches in the theft and loss of laptops. Only 6% of the cases were attributed to hacking and 2% to malware. “By count alone, hospital and physician practices are the most at fault,” accounting for 60% of the total. "Healthcare is one of the most targeted industries by hackers," said Hoala Greevy, Founder CEO of email encryption provider Paubox. "This makes it vital to close any security gaps as providers move to electronic records and new technology. Everything from sending an email to digitizing records needs to be addressed."

* [Thor Olavsrud, writing for CIO](http://www.cio.com/article/2384855/compliance/most-data-breaches-caused-by-human-error--system-glitches.html), “Most data breaches are caused by human errors and system glitches—application failures, inadvertent data dumps, logic errors in data transfer and more.”
* [Marion Jenkins, Ph.D. in Health IT & CIO Review said](http://www.beckershospitalreview.com/healthcare-information-technology/the-real-causes-of-hipaa-security-breaches-bad-it-system-design-bad-user-behavior-bad-policies-bad-operations.html) that the real causes of HIPAA security breaches are bad IT system design, bad user behavior, bad policies, and bad operations.

**Conclusion**

It would appear that blaming HIPAA security rules for data breaches only shifts the blame. But, given how comprehensive the privacy and security rules are, the challenge presented is broad and deep.

Time and cost-intensive as security management may be, covered entities must champion patient privacy and protection. They have to make the principle and process part of the organization’s culture. And, they must prioritize risk management and loss prevention because it is the right thing to do.