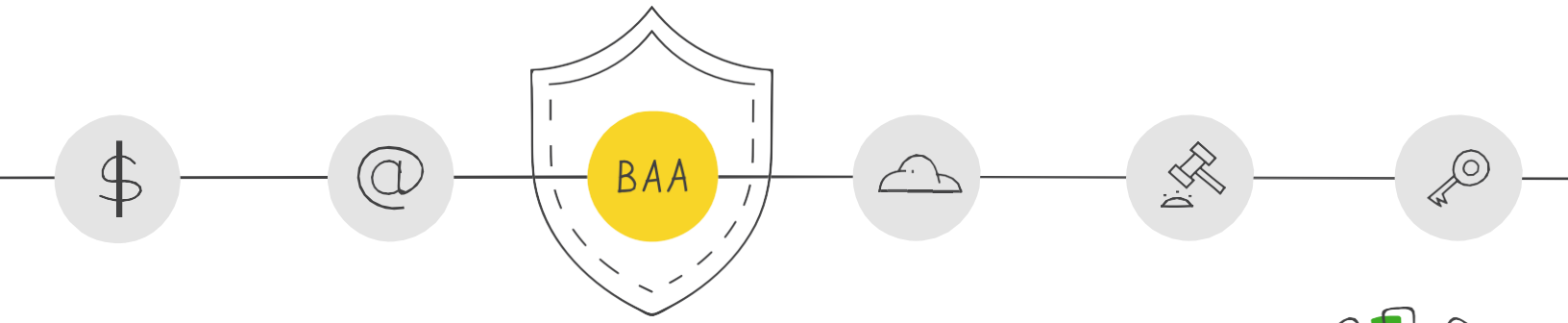
Phone.com
Communicate Better®

UNDERSTANDING INTEROPERABILITY & SECURE, COMPLIANT COMMUNICATIONS IN HEALTHCARE

What's Inside

In an interview with HealthITSecurity.com, Indiana Health Information Exchange (IHIE) Vice President, General Counsel, Privacy Officer **Valita Fredland** commented:

> More healthcare data and a higher degree of interoperability between provider systems, HIPAA covered entities will need to form partnerships with other organizations to ensure the security of their data assets. These partnerships are known as business associate agreements (BAAs).



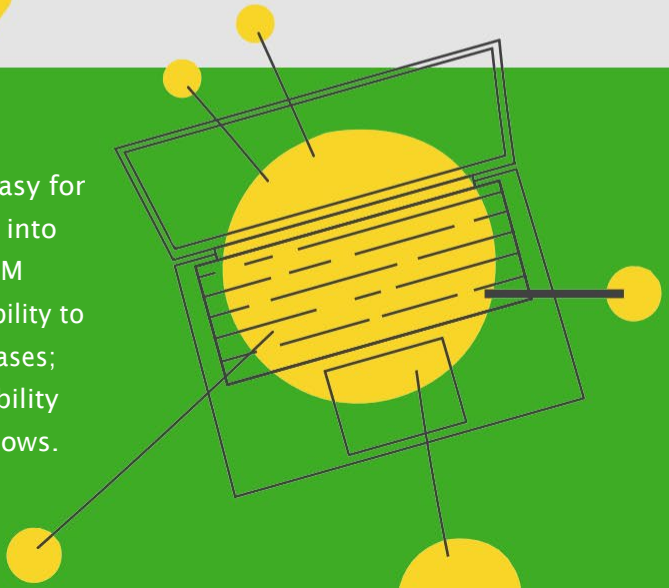
Reward

The population health and accountable care initiatives will also benefit from improved interoperability, and having health data be more readily available.

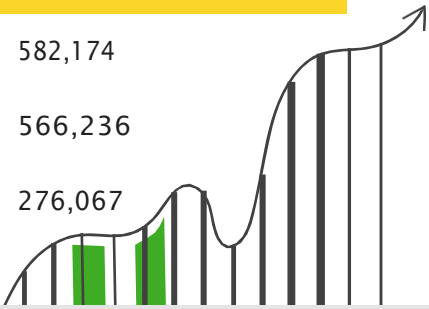
Risk

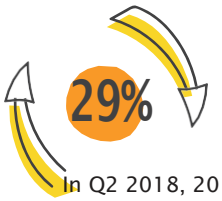
But for the information to be made available, it will be exchanged across a legal landscape that has varying degrees and various levels of privacy and security rules and regulations. Organizations responsible for compliance with HIPAA and HITECH need to ensure the same privacy and security compliance with interoperability exchanged data, as with their other sensitive data.

Phone.com's lightweight APIs make it easy for small businesses to extend UC services into third-party portals, middleware, and CRM platforms. Further, they provide the flexibility to create new applications for specific use-cases; custom integrations remove interoperability issues that complicate and delay workflows.

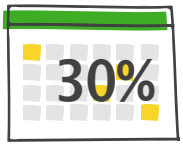


Q2 2018 largest health data breaches	Organization Type	Type of Breach	Number of Affected Patient Records
April	Agency	Theft	582,174
May	Provider	Hacking	566,236
June	Business Associate	Hacking	276,067

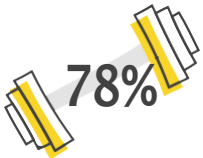




In Q2 2018, 20 percent of privacy violations were by repeat offenders.



If a healthcare employee violates patient privacy once, they are more than 30 percent likely to do so again within three months.



78 percent of clinical and non-clinical employees lack training of staff lacked proper data privacy and security awareness.

Insiders continue to repeatedly breach patient privacy

In Q2 2018, 29.71% of privacy violations were repeat offenders. This evidence indicates health systems accumulate risk that compounds over time if proper reporting and education do not occur. On average, if an individual healthcare employee breaches patient privacy once, there is a greater than 30% chance that they will do so again in three months, and a greater than 66% chance they will do so again in a year. In other words, even minor privacy violations that are not promptly detected and mitigated, have the potential to compound risk over time. Routine training and education are instrumental in preparing healthcare employees to prevent common threats to patient privacy. A study conducted in early 2018 found that 78% of staff lacked proper data privacy and security awareness. Resources provided to healthcare organizations are pivotal in reducing the number of breach incidents that occur. Educating and retraining workforce members on data privacy and security policy and procedures can reduce the frequency of repeat offenders within the organization.

[1] Protenus Breach Barometer

Joel Maloff, HIPPA Compliance Officer & SVP of Strategic Partnerships, Phone.com

"We've ensured that any patient information is encrypted and that all of our employees are trained in compliance.

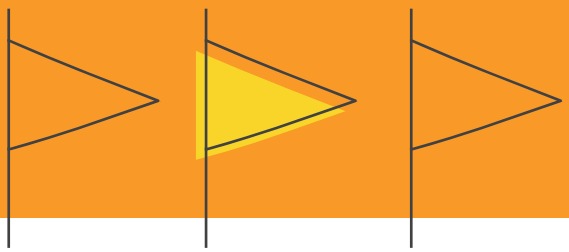
Insiders continue to repeatedly breach patient privacy

HIPAA compliance in a post-GDPR digital age creates hot button issues with gray area compliance criteria. Even if management teams are currently passing all HIPAA checks, patient information shared by voicemail, MMS or text message in the past may pose delinquency and security risks. Many times, these risks can come from poor governance of employee-patient communications and termination.

Scenario 1

An administrative employee named Ted works for Dr. Smith, a semi-retired private-practice pediatrician, and is the primary point of contact for patients, other doctors, accounts receivable and insurance billing, may unintentionally expose granted information in a risk-inducing manner.

If Ted leaves Dr. Smith's practice, which in this case is the "covered entity", **he may still have sensitive data in his possession.** A text notification or recorded voice message left on Ted's mobile phone from a patient with whom he's worked for years may seem harmless, but these communications are considered private patient information (PPI). If there is no segregation between Ted's phone and the PPI, there is a high probability that HIPAA laws will be broken.



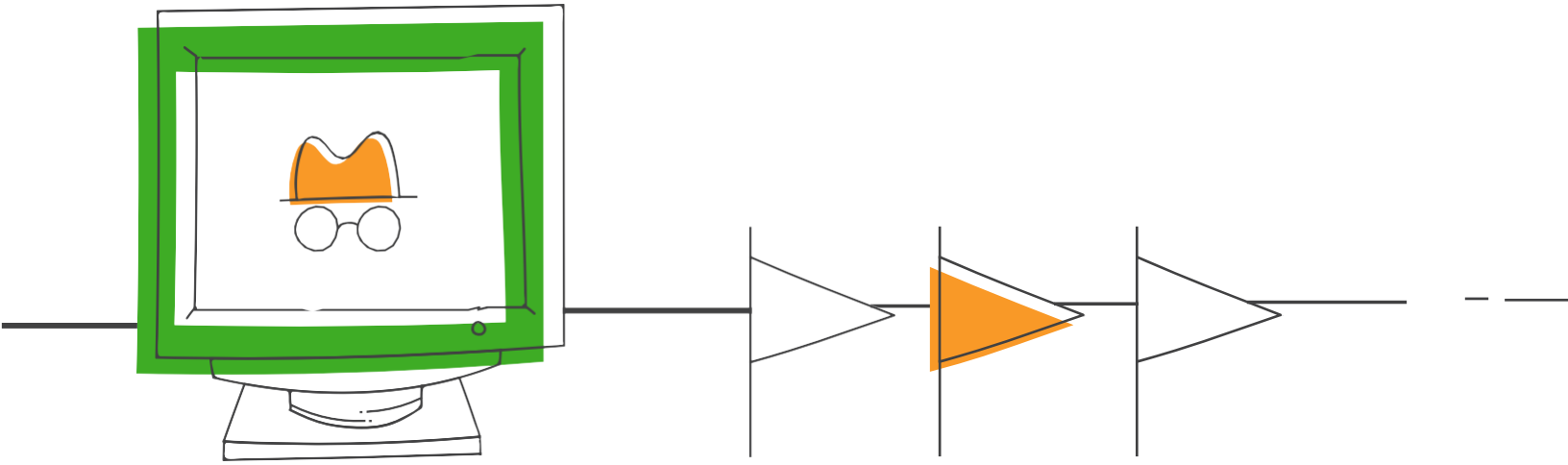
John Shegerian, Co-Founder and Executive Chairman, ERI

Hardware hacking in particular is an area that an alarming number of organizations are simply not prepared to confront.

Even if 'wiped of data' in the traditional sense, computers, cell phones, tablets and other devices used in medical scenarios, at the end of their life cycles pose a massive risk. Because the technology that organizations use may contain components that store sensitive information, health-related organizations must take this problem very seriously to avoid exposure and potential HIPAA regulation violations.

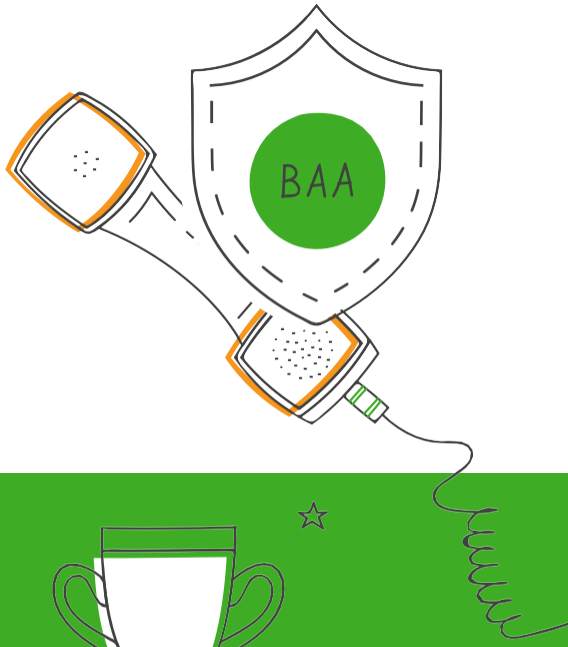
Russell Jones, Risk and Financial Advisory Partner, Deloitte & Touche LLP

Legacy devices can have outdated operating systems and may be on hospital networks without proper security controls.



Business Associate Agreements

Why you need one. Why you want one.

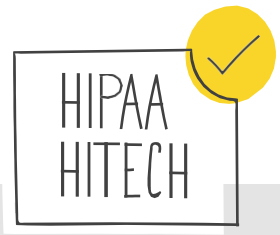


According to HIPAA privacy experts, a lack of Business Associate Agreements is a common violation. HIPAA and HITECH are regulations governing medical data privacy. Healthcare professionals are required to safeguard patient Medical information and a compliant, secure phone system is one part of that requirement.

For channel partners, agents, managed service providers and integrators, partnering with Phone.com provides a distinct business benefit that is valued by healthcare providers and sets them apart from competitors.

If your organization works within healthcare, understanding the demands of HIPAA and HITECH are important. These regulations can have a direct impact on your ability to serve these customers with confidence.

Voice communications includes several areas in which Protected Healthcare Information (PHI) may be exposed, such as voicemail, call recording, fax, or SMS, text, and MMS messages.



Hospitals, clinics, caregivers, and businesses that support healthcare practitioners such as billing, software, and management services **are all subject to audits for HIPAA compliance.** That means that their phone service providers must be compliant as well.

To protect our customers who work with healthcare providers from violating HIPAA laws, Phone.com offers a secure, cloud-based business communications service that is compliant with both HIPAA and HITECH standards.

Joel Maloff, HIPPA Compliance Officer & SVP of Strategic Partnerships, Phone.com

Storing and recording information such as voicemails and calls make communications a compliancy issue. Unlike most of the larger VoIP companies, we took the necessary steps to protect our current and future healthcare clients.

Are there risks for non-compliance? Absolutely!

>1000

Healthcare organizations – referred to as Covered Entities (CE) – risk **substantial fines** if found to not be compliant by a HIPAA review.

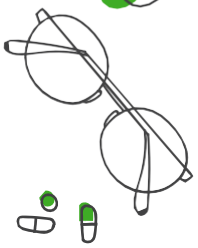
Organizations that provide services to Covered Entities, such as a phone service provider or billing company – known by HIPAA as a Business Associate (BA) – can also be fined if found to be negligent. Even for small and medium-sized businesses that cannot afford in-house compliance officers, the risk is ever-present.

More than 1,000 healthcare providers across the U.S. and Canada trust Phone.com to ensure their business communications are HIPAA-compliant. In less than 1 year, more than 400 service providers, vendors, and other companies have taken advantage of our HIPAA-compliant and HITECH-compliant services to expand their reach.

BYOD (Bring Your Own Device)

A study published in the **Journal of Hospital Librarianship** estimated that 85 percent of healthcare professionals were bringing their own devices to work.

Other issues arise when a patient's information is communicated using personal devices via BYOD or, "bring your own device", policies. In addition to numerous nightmare scenarios and compliance issues with the devices, information passed through non-encrypted channels increases hackability ratio. Many people do not use encrypted communications in their day-to-day comings and goings. Even those who use VPNs are still subject to sulnerabilities created by the VPNs themselves.



According to the **Journal of Hospital Librarianship**, an estimated 85% of healthcare professionals also engage their own devices at work. This puts the risk back on the hospital itself. Hospitals on tight budgets often fail to replace legacy equipment as it becomes outdated. With obsolete operating systems, hospital network devices are left exposed, "without their proper security controls", to cite Russell Jones of Deloitte Risk and Financial Advisory Department, Deloitte & Touche LLP.

Caregivers who use their personal devices in a clinical setting can be particularly problematic.

Scenario 2

Suppose Dr. Smith, Ted's former boss, is on vacation and uses his wife's iPhone to review an x-ray sent by a physician covering his patients while he's away. Like many of us, Mrs. Smith has her phone set up to save and automatically download every image received, and the x-ray gets lumped in with the vacation photos that auto-post on Facebook. By removing this private patient information from an encrypted environment, Dr. Smith has made his patient's x-ray accessible to a simple hack like was just reported about Facebook messages.

Mrs. Smith could also lose her phone without having deleted the patient's x-ray or the related correspondence between the two physicians. In either case, the information is not only open to hackers, but to anyone who finds her phone. As severely sensitive information has slipped through the cracks, albeit unintentionally, Dr. Smith and his colleague are now vulnerable to malpractice allegations of mishandling patient information.

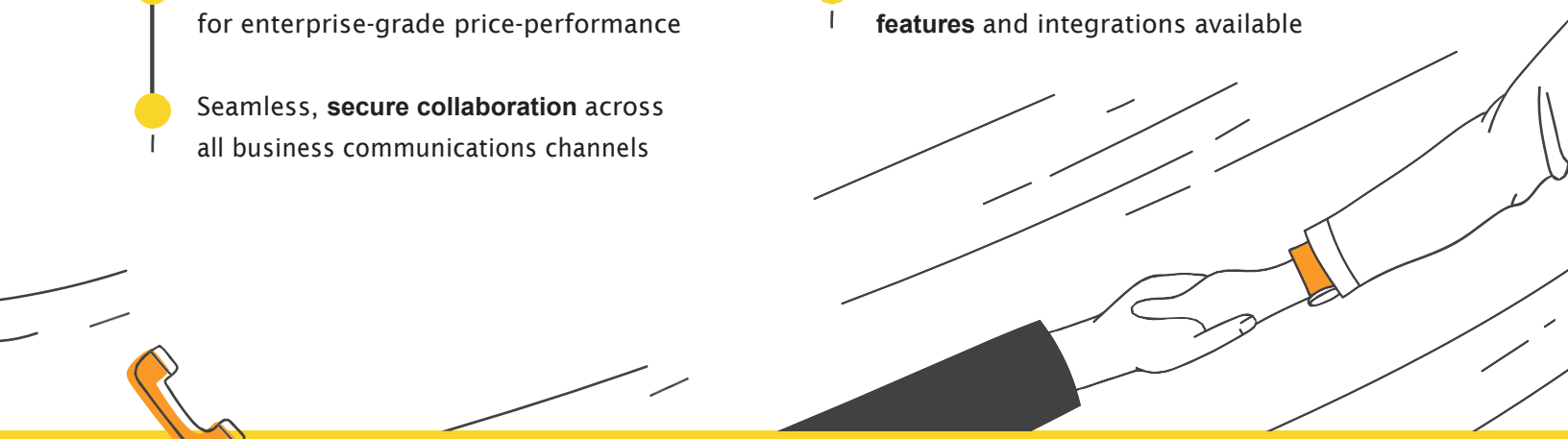
Identifying the criteria of these gray area HIPAA risks will protect both caregivers and the companies with whom they conduct non-clinical business from severe legal implications caused by associative guilt.

For a small business found to have violated HIPAA regulations, the cost of non-compliance can be dire. To HIPAA auditors, **ignorance is not an acceptable excuse**. Both covered entities and their business associates must be dilligent, fully aware of and responsive to HIPPA requirements.

Are you and your suppliers capable of passing a HIPAA audit?
Contact us today to secure your Business Associate Agreement.

Founded in 2007, Phone.com is the leading authority on cloud-based unified communications for business. Today, more than 30,000 businesses and 400 channel partners across the U.S. and Canada use Phone.com.

- **Award-winning**, US-based customer support regularly honored for QoS, reliability and business continuity
- **6 straight years** on INC. 500 Named
- to Deloitte Fast50 delivering for enterprise-grade price-performance
- Seamless, **secure collaboration** across all business communications channels
- Extensible UCaaS platform built on the **Amazon Cloud**
- API-enabled custom integrations for specific workflows
- **Over 50** customizable business communications **features** and integrations available



For small business owners and entrepreneurs who need communication systems that are flexible, convey brand professionalism, and support remote and mobile employees, Phone.com provides a complete portfolio of cloud-based UC&C and enhanced business services that make it seamless and easy to communicate **by any channel, from any location, on any device.**

Unlike big telcos and cable operators, Phone.com's UCaaS suite **delivers voice, video, fax, conferencing, collaboration**, and numerous other enterprise-grade services without suffocating long-term contracts or obsolete technology that stifle performance and innovation.

HEADQUARTERS
625 Broad Street,
Suite #240
Newark, NJ 07102

CORPORATE: 973-577-6380
SALES: 800-842-3394
EMAIL: sales@phone.com

Phone.com
Communicate Better®