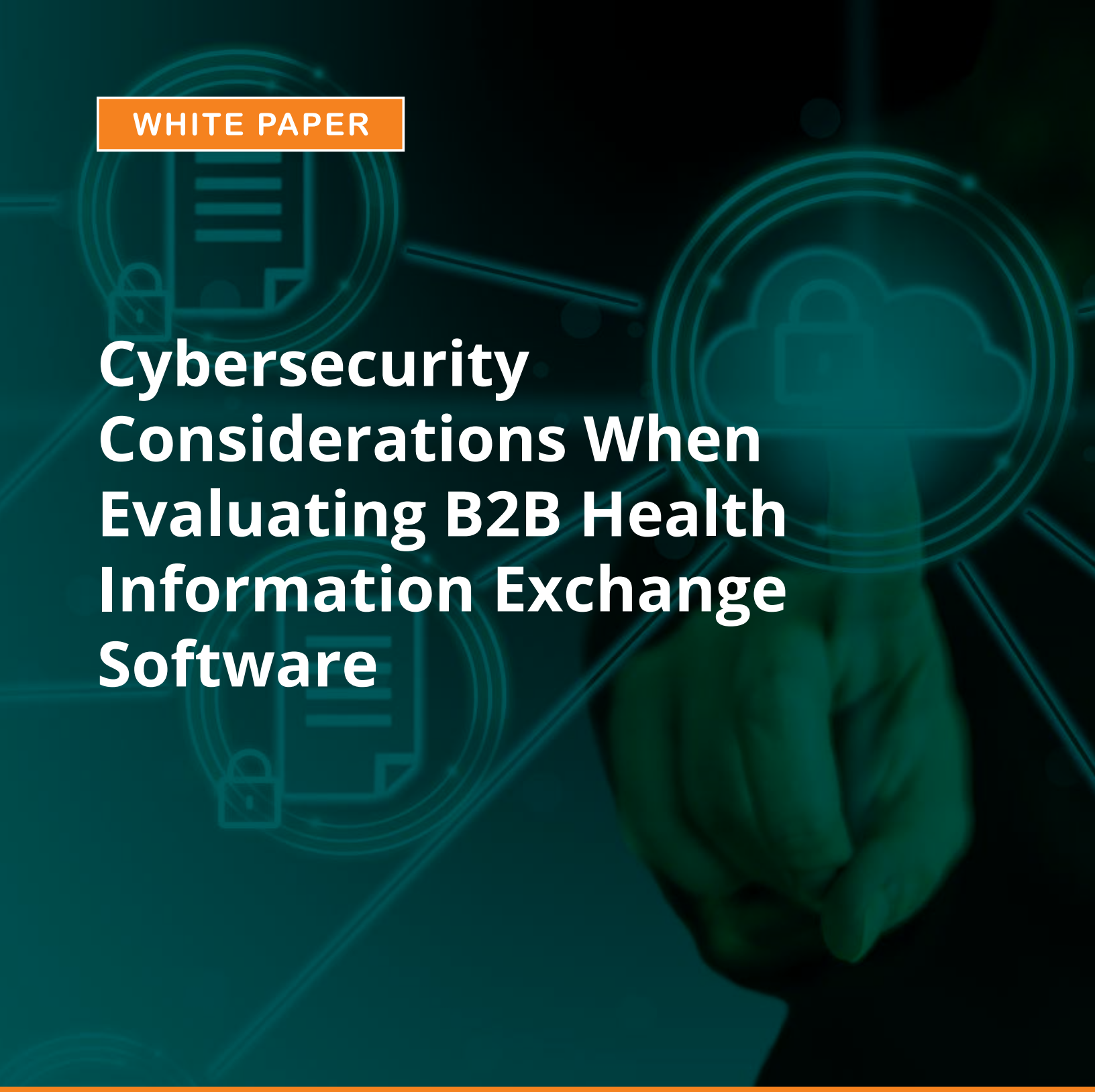
WHITE PAPER

Cybersecurity Considerations When Evaluating B2B Health Information Exchange Software



ChartSwap™

HIPAA COMPLIANT

AICPA SOC
aicpa.org/soc4so
SOC for Service Organizations: Service Organizations™

The past decade of the post Electronic Health Record (EHR) era brought tremendous advances in the pursuit of the digital transformation's famed potential. Even still, the subject creates a great deal of cognitive dissonance for the risk-averse industry. Across the ecosystem there is enormous pressure to rein in costs and improve efficiency--both underpinnings of the digital transformation--yet healthcare continues to lag behind other industries when adopting digital strategies and innovative technologies.

One area that evades even the most entrenched foot-draggers is the metamorphosis of the traditional, and highly manual Release of Information (ROI) process. According to the 9th Annual Industry Pulse Survey[1], the use of health information exchanges (HIEs) rose sharply, demonstrating the important role in healthcare by facilitating the transfer of sensitive personal health information (PHI) between physicians, hospitals, payers, law firms, and other providers. Survey respondents using HIEs as a primary source of data doubled in just a year from 3.8% in 2017 to 9.1% in 2018. The growth demonstrated that electronic data exchange had gained a foothold. While encouraging, rapid adoption of any technology without proper evaluation can be harmful.

UP 200%

HIEs as a primary source of data doubled in just a year from 3.8% in 2017 to 9.1% in 2018

Digitizing the transfer of medical records, for better or worse, revolutionizes operations. If done right, it allows for a faster, easier, and safer exchange of health information. If done wrong, it can introduce more cybersecurity risk and present compliance challenges.

Moving to a B2B HIE Software is the First Step in Securing ROI

The traditional model of ROI is inherently insecure as provider organizations rely on outdated techniques that increase risk and jeopardize PHI:

Traditional ROI Processing Methods		Security Concerns
Routing Requests Using Paper or Unencrypted Email	→	**PHI Disclosure**
Paper Reminder Notes to Fulfill Requests	→	**Vulnerable Email Servers**
Unsecured Faxing	→	**Illegitimate Requestors & Recipients**
Postal Mail	→	**Stolen Postal Mail**
Tracking Using Spreadsheets or Public Drives	→	**Inaccurate or Nonexistent Audit Trail**

Given that traditional ROI processing methods have no security whatsoever and are ripe for human error, at a basic level, even adopting a 'less secure' integrated B2B HIE record retrieval software will decrease risk. Because HIEs send all activity through encrypted portals, it reduces the likelihood that cybercriminals can view or intercept data. And because HIEs involve the transfer of PHI, there is increased pressure to ensure that their networks are secure and in compliance with regulations such as Health Insurance Portability and Accountability Act (HIPAA).

Even Though HIEs Are More Secure, Not All HIE Cybersecurity Is Equal

According to the RSA Digital Risk Report[2], addressing cyber attack risks was one of the top priorities for healthcare organizations. This comes as no surprise as healthcare ranks in the top two industries to experience data breaches from cyber attacks.

Malicious actors view healthcare as a high-value target since individual medical records can sell for as high as $1,000[3] on the dark web. As digital strategies and the amount of digitally available patient data grows, provider organizations' digital footprints and attacks surfaces grow too. Meaning, there are more entry points and technologies to exploit and use for nefarious purposes—and more cybersecurity required.

When evaluating HIEs it is crucial to keep this at front of mind, and not only evaluate HIEs on criteria such as ease of use, but on the underlying cybersecurity and current security controls.

HIE Cybersecurity Features to Consider

For providers with limited or non-existent IT support, cybersecurity is often a foreign world. However, there are general security considerations that even security novices can and should strive to understand when evaluating B2B HIEs.

Inherent Security Infrastructure

Even if providers are not comfortable with the more detailed aspects of cybersecurity, it is wise to ask about the technological foundation of the B2B HIE platform. These details will allow providers to determine if the vendor developed the platform on well-established frameworks that already have proven technical security safeguards in place. This can be confirmed with a simple online search to verify the legitimacy and track record of the underlying technologies.

Encrypted Portal With Audit Trail

Because of the digital transformation, it is commonplace to manage and store vast amounts of personal information in the cloud and on servers. Portals should encrypt data, so even when transferred or stored, it remains secure.
During the process of encryption, patient data is scrambled so that only the receiver who has the secret code, or decryption key, can see its readable version. In addition, portals should have a detailed audit trail of who, what, and where were involved in the transfer of data so that illegitimate activity can be flagged and stopped.

Size of Network/Ecosystem

Not all cybersecurity considerations are purely technical. Good HIE companies will have an expansive network of providers and requesters. If providers choose a B2B HIE with a small network, it will force them to complete both digital and manual ROI transactions--essentially gaining only partial security value from going digital.

Storage of Files

For providers that worry about the liability of B2B HIEs, storage of records can be a big concern. Patient data travels out of the provider's network and into a B2B HIE's cloud or server, which can take control out of the provider's hands. There are several ways to overcome this. HIEs should offer encrypted data with:

- Precise tracking and detailed records of request fulfillment timelines
- Procedures and controls for automatic deletion after a specified period of time
- Ability to request file deletion and confirmation of successful deletion

Access to Portal

Some portals may require more difficult and risky deployments, including opening a port to a firewall. Providers, especially smaller provider organizations, would benefit from simple web-based solutions that only require a modern web browser to access the portal. Then, there is no need to have IT support to secure and gain access to the HIE.

Verification of Users

A common problem with digital transactions is illegitimate users masquerading as legitimate people or entities. HIEs should take additional steps to verify the identity of all users engaging in ROI transactions. This could include detailed research of publicly available information or phone calls to ensure the requestor's legitimacy.

Compliance

Compliance is becoming the expectation for the entire healthcare industry. As providers work to become more efficient by adopting digital strategies, they must ensure their third-party solutions strictly adhere to compliance frameworks, that include HIPAA & SOC II.

HIPAA

HIPAA compliance is one of the most pressing concerns for healthcare organizations and companies. All HIEs serve as a way to maintain HIPAA compliance in provider settings and they themselves should also have a record of compliance of backup, encryption, data integrity and storage, authorization and disposal.

HITECH

B2B HIEs should also be HITECH-compliant, which means the HIE follows the guidelines established by the Health Information Technology for Economic and Clinical Health Act (2009)--regulating the use of EHRs and electronic medical records (EMRs).

SOC 2 Certification

It is becoming increasingly common for organizations to request that their vendors become SOC 2 compliant to ensure they have strong security postures. Based on the Trust Service Criteria from the American Institute of Certified Public Accountants (AICPA), the SOC 2 framework is an auditing procedure that verifies that companies comply with one or more of the five trust principles based on the systems and processes in place.

5 Trust Principles

1. **SECURITY** – The protection of system resources against unauthorized access.
2. **AVAILABILITY** – Accessibility of the system, products, or services as stipulated by a contractual agreement of the minimum acceptable performance level for system availability.
3. **PROCESSING INTEGRITY** – Whether or not a system archives its purpose (i.e. deliver the correct PHI to the correct requestor).
4. **CONFIDENTIALITY** – If access and disclosure is restricted to a specified set of persons or organizations.
5. **PRIVACY** - The system's collection, use, retention, disclosure and disposal of personal information in conformity with an organization's privacy notice, as well as with criteria set forth in the AICPA's generally accepted privacy principles (GAPP).

By completing a SOC 2 certification, B2B HIEs demonstrate they continually review developments and threats as part of comprehensive security policies and procedures. This differs from HIPAA and HITECH because the audit determines the compliance by evaluating oversight procedures, a mechanism for alerts, audit trails, and actionable analytics.

For example, if a provider agrees to disclose patient information to a requestor after agreeing to a privacy policy, but the HIE routes it to the wrong requestor. The SOC 2 audit report would then include the privacy policy and the related process to ensure the vendor handled the data based on any committed or agreed upon policies.

Unlike HIPAA and HITECH which have very rigid requirements, SOC 2 reports are unique to each HIE organization so audits are in line with specific business practices. Because of this, no matter how HIEs define and implement their security and privacy practices, providers can feel confident that it is effective and compliant.

Enterprise-Grade Cybersecurity Providers Can Trust

As healthcare organizations continue to adopt digital ROI processing, selecting a security-first B2B HIE portal will be an essential factor in protecting from the damaging financial, reputational, and operational effects of data breaches.

In its effort to revolutionize the exchange of EHRs/EMRs, payments, and communications related to billing and medical records requests, ChartSwap is continuously working to improve its security posture. As a Trustwave Payment Card Industry Data Security Standard (PCI DSS) Certified organization and the first and only B2B HIE to achieve SOC 2 certification, ChartSwap guarantees an increased level of security for all PHI. Trusted by providers and requestors for thousands of daily transactions across the nation, ChartSwap built the web-based platform with security that is unparalleled by current HIPAA compliance standards in mind and continually audits for stringent privacy and data protection around the clock.

For more information on how the most secure B2B HIE in the industry can help your organization, please visit: chartswap.com and request a demonstration today.

References

1. 9th Annual Industry Pulse Survey

2. RSA Digital Risk Report

3. Healthcare IT News