cognizant®

Reducing payers' clearinghouse risk in the age of cyberattacks

In an era where digital transformation is reshaping healthcare, robust cybersecurity measures are essential. Protecting sensitive patient data and maintaining the integrity of technology is integral to maintaining business continuity and issuing proper reimbursements.

Cybersecurity attacks directed at healthcare organizations are on the rise. The HIPAA Journal reports that 2023 set records for the highest number of data breaches and the most breached records since 2009 when the Department of Health and Human Services (HHS) Office for Civil Rights (OCR) first mandated the data be published.[1] An incredible 725 data breaches were reported with 133 million records inappropriately disclosed. In 2024, there have been nearly 400 breaches reported so far, including the devastating Change Healthcare cyberattack orchestrated by BlackCat.[2]

For payers, these attacks have meant reassessing clearinghouse strategies, increasingly turning to decentralization to mitigate risk and add redundancy options to protect their business. Because clearinghouses act as a central connection between payers and providers, heightened security measures are an indispensable part of the business strategy.

[1] https://www.hipaajournal.com/healthcare-data-breach-statistics/
[2] https://www.aha.org/news/aha-cyber-intel/2024-10-07-look-2024s-health-care-cybersecurity-challenges

Choosing the right clearinghouse model for your business

There are multiple clearinghouse models from which to choose. Each has its own benefits, but ultimately the decision comes down to how your business functions and what your needs are in terms of risk mitigation.

Single direct connection

A direct connection is when a clearinghouse is directly connected to a payer and is made available to handle varying levels of transactions. The primary model for years was an exclusivity model that allowed the clearinghouse to act like a single middleman for all claims. Many payers are rethinking this strategy based on with the recent growth in cybersecurity threats.

Multiple connections

Payers are adopting a “one-to-few” model, using a few trusted clearinghouses to reduce direct connections. Choosing a model with two or three preferred clearinghouse minimizes the administrative burdens in managing multiple lines of business, while providing flexibility and reducing reliance on a single vendor.

Regionally-based exclusivity

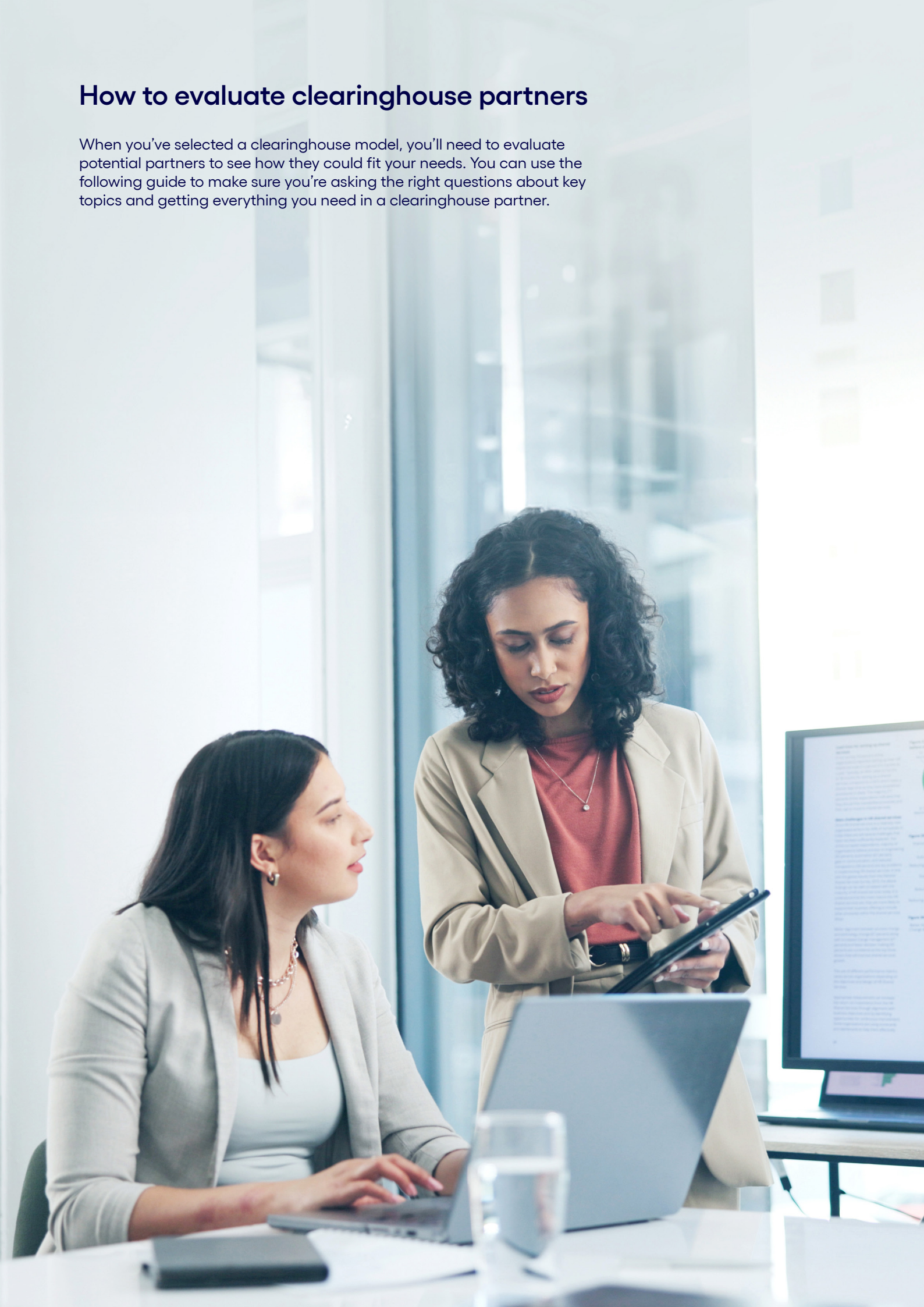
A regionally exclusive connection occurs when a clearinghouse is the exclusive connection for certain areas like a specific state. It uses the direct connect model for a subset of an organization’s claims, which allows for a quick alternative clearinghouse option if there’s a problem with another one of the payer’s clearinghouse partners. Many businesses choose to have two or three regional clearinghouses.

Redundancy option

Having a clearinghouse as a redundancy option means there’s a connection between the clearinghouse and payer, but claim volume isn’t guaranteed. The redundant clearinghouse acts as a backup system in case the primary clearinghouse fails or has a major problem.

How to evaluate clearinghouse partners

When you've selected a clearinghouse model, you'll need to evaluate potential partners to see how they could fit your needs. You can use the following guide to make sure you're asking the right questions about key topics and getting everything you need in a clearinghouse partner.



01 Dedicated account management

Dedicated account management means that a clearinghouse partner offers direct one-to-one or dedicated team support to assist their payer partner more quickly and efficiently than waiting in a long call queue. It provides the ability to be flexible, often including scaled pricing and/or bespoke options based on what the partner needs.

One element of a dedicated account management model might include a centralized gateway for all of a payer's clearinghouse connections, which improves claim processing rates and creates a higher clean claims submission rate.

Questions to ask a potential clearinghouse partner:

Does the partner offer direct support? Or will you have to call into a call center?

Does the partner maintain and distribute companion and training guides to the plan's providers?

How does the partner accommodate payer-specific needs?

Is the partner able to support the plan's providers through direct claim entry portals?

02 Onboarding and operations efficiency

Being able to collaborate and work cohesively is a key part of any partnership, especially a clearinghouse. Before this work begins, however, you'll need to know about the onboarding process and how long the solution will take to implement. Then, once it's live, how it will create efficiencies in the workflows you already have in place. The best partner will be able to thoroughly demonstrate how working with them will help you better your processes and strengthen your operations strategy.

Questions to ask a potential clearinghouse partner:

As a payer, how could I use custom edits to make the inbound claims review and reject process more efficient?

What actions does the partner take for proactive paper claim reduction?

Is an enrollment portal available to streamline front-end processes?

03 Security

Payers and clearinghouses parse an incredible amount of data, which makes security paramount. Having a secure connection and strategy for protecting sensitive data is a HIPAA law requirement, which means it's critical for safety measures and legal compliance.

As the amount of data has increased, so too have the measures to protect it. There are scans, practices and certifications you should ask about with every potential partner, especially one that will be as connected to your data as a clearinghouse.

Questions to ask a potential clearinghouse partner:

What security certifications does the partner hold?

- HITRUST
- EHNAC
- CAQH CORE
- SOC 2

What security standards does the partner follow?

- Do they offer and administer regular training?
- Do they have a regularly tested business continuity plan (BCP)?
- What policies and procedures are documented? Are they kept up to date?

Does the partner use multifactor authentication? If so, how?

Does the partner use third-party risk assessments? If so, which ones and how are they completed?

04 Reporting

When so much data is involved, excellent recordkeeping and reporting practices are essential. Ample reporting capabilities allow you to meet the numerous federal agency compliance requirements, as well as keeping a keen eye on what's happening within your organization.

In a clearinghouse partner, the ability to create custom reports can help you monitor transaction volumes, gauge overall system performance and strategically plan for the future of the business.

Questions to ask a potential clearinghouse partner:

How does the partner handle reporting?

What's the reporting cadence?

Are there customized reporting options available?
(For example, volumes by provider or payer rejection types)

Cybersecurity is changing the way healthcare looks for everyone, especially those facilitating payments. There are clearinghouse model options on the market today that can allow your business to be simultaneously more secure and more flexible. If you're in the market for a new or additional clearinghouse partner, make sure you're considering your risk mitigation and asking the right questions so you can make the best decisions for your business.

World Headquarters
300 Frank W. Burr Blvd.
Suite 36, 6th Floor
Teaneck, NJ 07666 USA
Phone: +1 201 801 0233
Fax: +1 201 801 0243
Toll Free: +1 888 937 3277

European Headquarters
280 Bishopsgate
London
EC2M 4RB, England
Tel: +44 (01) 020 7297 7600

India Operations Headquarters
5/535, Okkiam Thoraipakkam,
Old Mahabalipuram Road,
Chennai, 600 096 India
Tel: 1-800-208-6999
Fax: +91 (01) 44 4209 6060

APAC Headquarters
1 Fusionopolis Link,
Level 5 NEXUS@One-North,
North Tower, Singapore 138542
Phone: +65 6812 4000

WF3151200