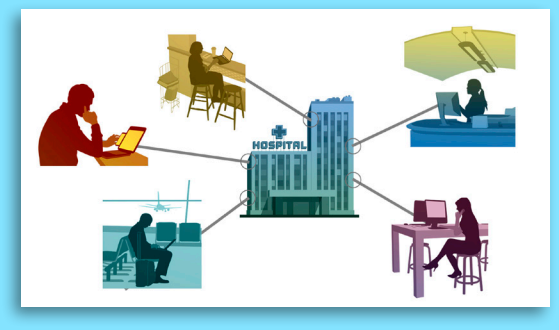
iatricSystems®

Prevent Third-Party Breaches, Protect PHI, and Avoid the "Wall of Shame" with iatricSystems SecureRamp™

Many hospitals have hundreds of business associates and other third parties accessing their systems remotely. Keeping track of them — and all their staff and subcontractors — is extremely difficult. Some things you should know about your partners:

- Are they protecting their devices from viruses and other malware?
- Are there dangerous weaknesses in their internal networks?
- Are the people accessing your protected health information (PHI) authorized to do so?
- Is a Business Associates Agreement (BAA) in place that specifies what they can access, and what for?
- Is the BAA up-to-date?

It's simply impossible to know for sure whether every third party has the training, resources, and time to keep track of all these details. For hospitals, the result is a huge exposure risk — of sensitive data, identity theft, crippling viruses, and having their systems held for ransom. These breaches come with a steep price: fines...ransom payments...being listed on the OCR "Wall of Shame" breach website...having to notify patients that you've betrayed their trust... lost revenue when they go elsewhere.



Unfortunately, third-party breaches occur constantly. Here are just a few examples:

Hospital Systems Held for Ransom

One hospital in the Northeast paid a $55,000 ransom to regain access to its computer systems. An investigation revealed that a hacker gained access to hospital systems using the hospital's remote-access portal, logging in with an outside vendor's username and password.

- ***With multi-factor authentication and other security measures, the breach could have been prevented.***

Hacker Accesses a University's Health System for 19 Months

A hacker breached one university's health system, infecting physician devices with malware that gave the hacker access to medical records of 1,882 patients for 19 months. Data impacted included patient names, diagnoses, treatments, DOB, and addresses.

- ***Increasing security by requiring updated antivirus on all devices that remotely connect to the network could have blocked and reported the attack.***

Pediatric Practice Fined for No BAA

One Illinois-based small pediatric specialty practice was fined $41,000 by the OCR in April 2017 for failing to obtain a Business Associate's Agreement.

- ***If the hospital had known the agreement was not in place, it could have alerted the practice before the problem was found in an audit.***

Subcontractors Breached, 19,000 BCBS Members Have PHI Exposed

A data breach involving two subcontractors of Blue Cross Blue Shield exposed personal information of about 19,000 plan members. According to the state insurance regulators, the breach occurred as the result of a ransomware attack.

- ***More effective network monitoring and access control (such as using Multi-Factor Authentication) could potentially have prevented the breach or caught it much sooner.***

To protect patient data, you need safeguards that extend to your third-party vendors and remote employees. That's why we developed SecureRamp™.

Secure Remote Access to Your Systems and Your PHI

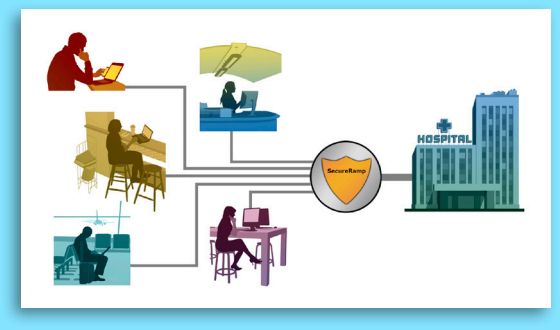
iatricSystems SecureRamp manages and simplifies remote access to your systems by third parties, reducing the risk of unauthorized access and malware attacks while saving time for your staff. Advanced security technology provides the monitoring and control you need when hundreds or thousands of remote users are accessing your systems daily. SecureRamp:

- Monitors the devices used to access the hospital's network remotely to ensure that antivirus, encryption, automatic updates, and firewall are in place and up-to-date.
- Can ensure that business associate agreements are in place and up-to-date, and restrict access if they aren't.
- Prevents unauthorized remote access by enforcing multi-factor authentication that requires additional evidence.
- Provides a single secure portal for all third-party access, rather than multiple (and possibly unsecured) remote entry points.

What Healthcare CIOs are saying about third-party security and SecureRamp:

- "We are not doing a good job of managing vendor connections. A solution like this would be a great way to manage vendors."
- "The [regulatory agency] has expressed interest for hospitals to have information about their vendors' networks and security protocols."
- "Current solutions — or lack of them — aren't in the best interest of our hospital or security in general."
- "With the OCR focusing on Business Partners, there is an increasing gap for hospitals that isn't filled with current technology or staff."
- "This would increase security for many hospitals."

Make third-party access safer — protect your systems, your patients, and your hospital with SecureRamp.



iatricSystems®

Ph: 978.805.4100 Fax: 978.805.4101 info@iatric.com secureramp.iatric.com