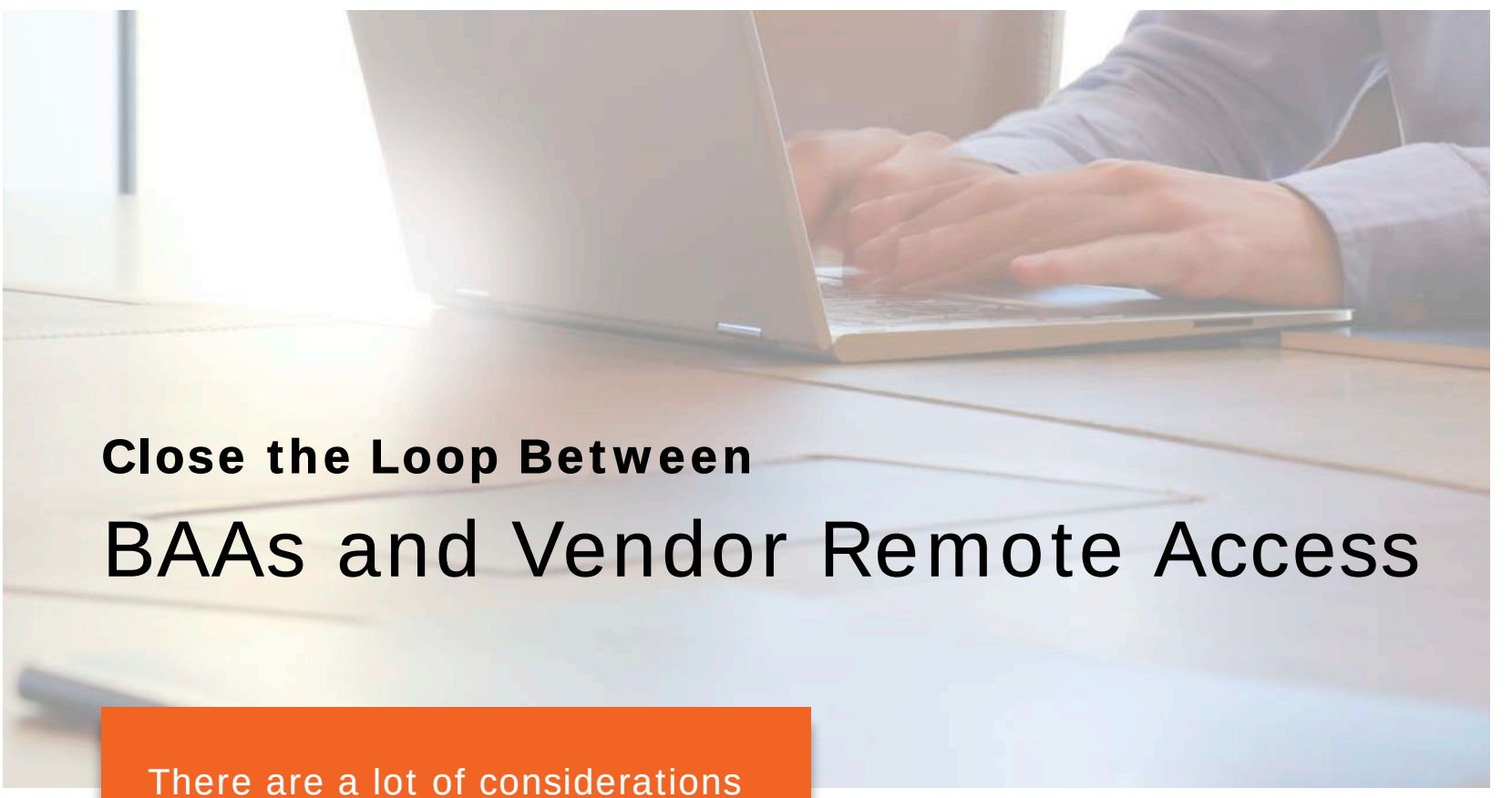
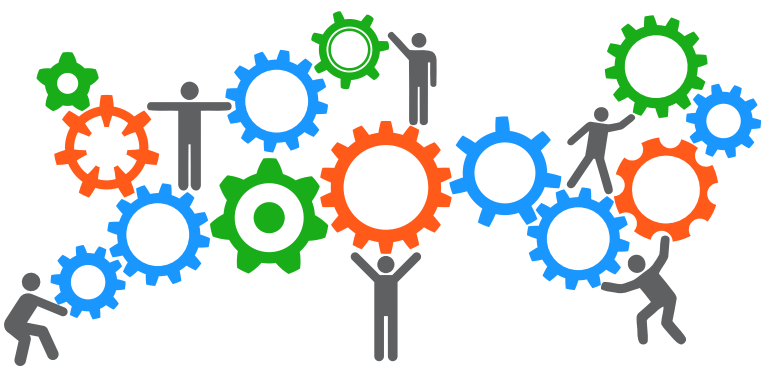


Close the Loop Between

BAAs and Vendor Remote Access

There are a lot of considerations when executing a BAA and vendor agreements, including how to provide remote access for valid agreements. Here are some questions to ask yourself to gauge the effectiveness of your current process:

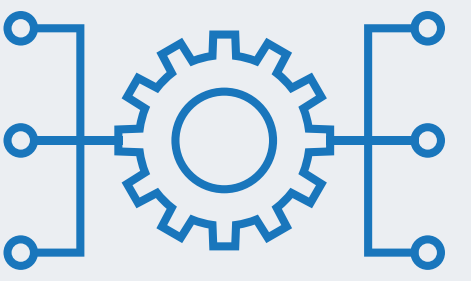


- ✔ Can you check each remote access attempt for a valid BAA?
- ✔ Does your IT Dept know when a contract and its BAA has expired, or is up for renewal?
- ✔ Do you have an automated process for the Compliance Department to let the IT Dept know when a contract is executed and it's ok to give a vendor access to the network (ie. The BAA is signed)
- ✔ Do you have an automated process for the Compliance Department to let the IT Dept know when a contract is terminated, and any access is to be disabled?
- ✔ How are you validating that you meet the HIPAA requirements of checking each vendor remote access to make sure they have a BAA in place?
- ✔ Would you pass an OCR audit (can you document that you check for a valid BAA)?

Compliance Team BAA Management and Hand-off to IT

Automating the process of providing secure remote access, and ensuring valid agreements are in place will make your networks more secure, and protect PHI. Here is an example of the automated process using a tool like SecureRamp:™

1. Contract is negotiated, reviewed and approved by both parties (Vendor and Hospital), including the Business Associate Agreement (BAA) and pertinent information is given to IT for remote access to ePHI.



2. Vendor information and BAA dates are entered in SecureRamp by Compliance. Compliance (or IT) notifies Iatric Systems to establish VPN. Vendor is set up in SecureRamp, IT adds designated remote users, creates a specific remote user group for that vendor, assigns appropriate server for that vendor to access, and sets any other IT rules within SecureRamp. SecureRamp will then automatically:

   a. Check each remote access attempt for a valid BAA
   b. Provide a warning to the user if the BAA is close to its renew date
   c. Email designated administrators at the hospital when an BAA is close to its renew date
   d. Block users from accessing the network if a Valid BAA is not on file, or is out-of-date
   e. Block remote users if their PC does not meet the required guidelines (rules) set within SecureRamp, such as Firewall not enabled, hard drive not encrypted, automatic updates not enabled…
   f. Notify designated administrators at the hospital when an end user is blocked from network access because of BAA not on file, or BAA is out-of-date
   g. Full reporting and audits showing user access
   h. Note: SecureRamp does not replace the contract management system, and the BAA is not housed in SecureRamp, just the pertinent dates and vendor information.

You are ultimately and always responsible with overseeing that the BAAs are in place and that remote access management is occurring. Third party breaches are on the rise. Here are a few examples of vendor breaches:

Third party breaches are costly!

1. Ponemon Institute reported that 56% of respondents experienced a data breach caused by one of their vendors, in 2017.
2. Third Party Vendors are behind 20% of Healthcare data breaches in 2018
   a. 23 percent of vendors assessed in a recent report represented a medium- to high-risk to the healthcare organizations to which they're contracted – many of which lacked the processes to adequately address risks.
   b. Specifically, of those in the medium- and high-risk categories:
      i. 17 percent were lacking in risk assessment
      ii. 12 percent in data security
      iii. 10 percent in governance
      iv. 9 percent in identity management and access controls
3. Third party breaches are costly!
   a. The American Journal of Managed Care reported in December 2018 that hospitals spend 64% more annually on advertising after a breach over the following two years.