INDUSTRY GUIDE

How to stay HIPAA compliant

with AP & AR automation

Automating Accounts Payable (AP) and Accounts Receivable (AR) through a software-as-a-service (SaaS) solution has become an indispensable tool for organizations in streamlining their back office.

However, for in the healthcare industry, HIPAA compliance is also critical for safeguarding patient information throughout all processes, including AP & AR operations.

How can organizations ensure HIPAA compliance when using an automated AP & AR SaaS solution?

HIPPA compliance

HIPAA is a federal law designed to, among other things, protect sensitive patient health information from being disclosed without the patient's consent or knowledge. This means ensuring that all aspects of patients' electronic protected health information (ePHI) are handled appropriately to keep that information private and secure.

Protected information includes just about any personal information related to a patient, such as their name, addresses, health condition, and any aspect of their medical care. In today's digital world, patient privacy and keeping ePHI private have become paramount.

To maintain HIPAA compliance, organizations must ensure their tools and applications provide protection for their ePHI, including their AP & AR automated solution. That solution should provide safeguards for protecting patient information, enabling organizations to remain HIPAA compliant.

Why is HIPAA compliance important in AP & AR automation?

HIPAA extends to almost every aspect of the healthcare process, including billing and invoicing. Patient data often extends into the AP & AR process, well beyond the physician's record of an office visit or diagnosis. For SaaS-based AP & AR, safeguarding your patient data is especially important given that the data entered into the application is stored in the cloud and managed by the vendor, not within the perimeter of your organization's data center.

ePHI is often included in invoices and payments. For example, patients often pay upfront costs that are later paid or covered by their health insurance, resulting in an overpayment to the healthcare provider that needs to be refunded to the patient. That refund becomes part of the AP & AR process.

Similarly, invoices from laboratories often contain patient information to correlate those services with a particular patient. The patient name and services contained in the invoice are considered ePHI. They must be secured and kept private from unauthorized access.

How do organizations stay HIPAA compliant with AP automation?

While the list of requirements for HIPAA compliance will continue to evolve, there are several key steps to help your organization stay HIPAA compliant when using an AP & AR automation SaaS-based solution.

Business Associate Agreements (BAA)

What is a BAA? A BAA is a contract that establishes your software vendor, or other third-party vendor, as a "business associate" under HIPAA in relation to your organization. The BAA should define how the vendor will safeguard electronic "Protected Health Information" ("ePHI") that your organization may upload or transmit with the software.

What does signing it mean?
Signing a BAA can establish the roles and responsibilities for you and the service provider for the joint protection of ePHI and also establish that safeguards are in place to meet recommended HIPAA guidelines in the security and privacy of the ePHI.

Data access

When it comes to ePHI, it's imperative that only those with the right privileges have access, applying and maintaining appropriate restrictions on the ability to view and edit that data. Be sure your AP & AR automation solution includes safeguards throughout the application where you, as the user, can put in place security privileges for what data, including ePHI, your staff, approvers, and management can view and edit.

For example, as part of your AR process, customers should only be able to view and pay invoice documents containing ePHI through a secure payment portal.

Other examples of data access protection include ensuring documents containing ePHI are not sent via email without additional protections to ensure end-to-end encryption. Email without these additional controls is not considered a safe and protected transmission method for ePHI.

Data access also applies to your AP & AR vendor. A BAA can help ensure that your AP & AR vendor has trained their staff and has taken security measures with their own personnel to ensure ePHI from your organization is kept private and secure.

ePHI designated fields

An AP & AR solution that supports HIPAA compliance will include specific fields designated for ePHI protection. Since ePHI needs to be kept private and secure, the handling of that data is particularly important. Limitations are put around the data in terms of who is able to access it and view it, as well as how it is stored and transmitted.

Encrypted data at rest

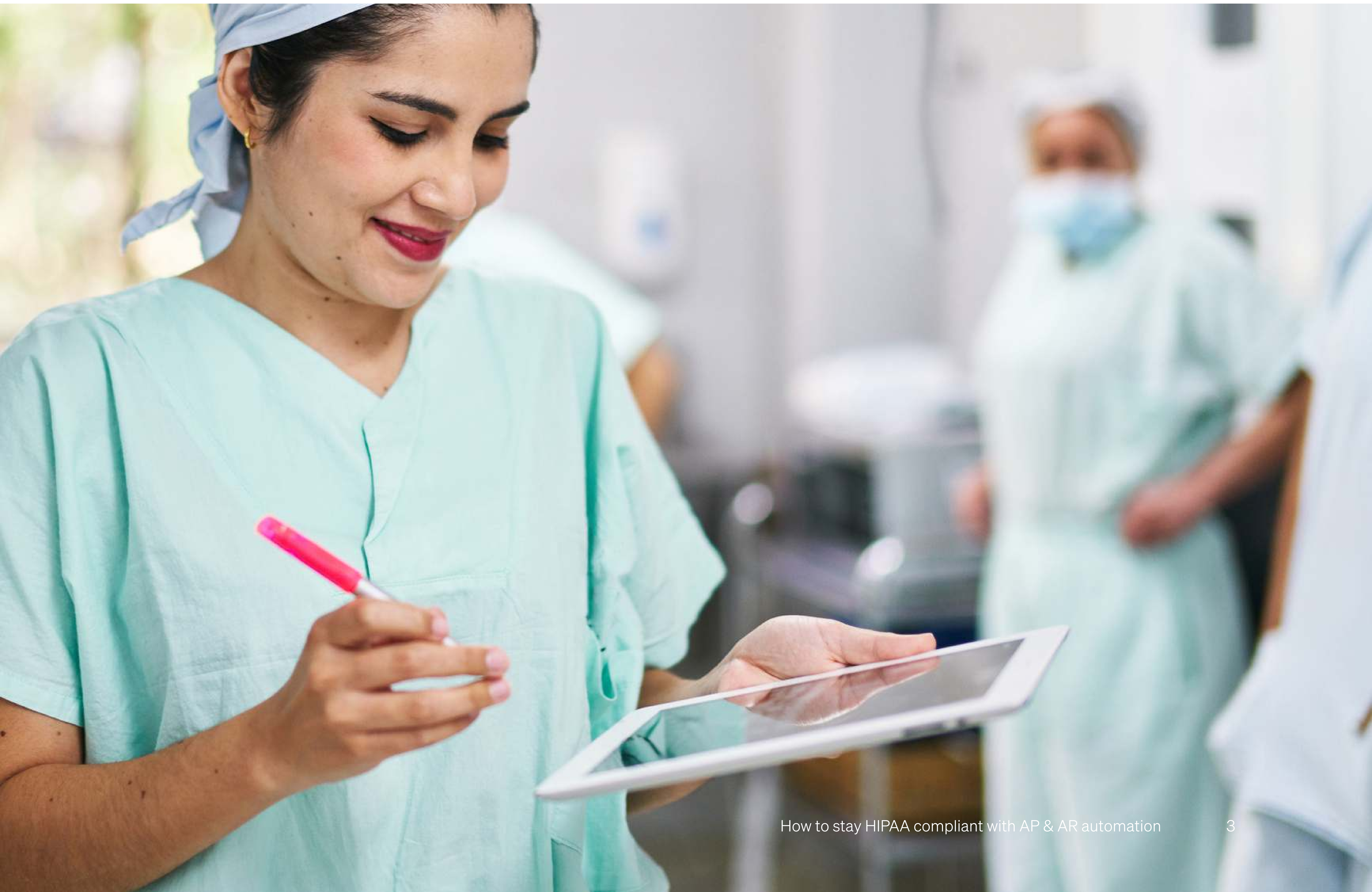
Your AP automation vendor should put safeguards in place for ePHI such as ensuring your ePHI (in the designated fields) is protected when stored on their system. This means ensuring the ePHI at rest is encrypted, so that if the servers in which the data is stored were ever compromised, the data could not be easily read or decrypted.

Encrypted data in transmission

Similarly, when the ePHI is in movement over an unprotected communication channel, like the public internet, that data should be protected and secured during transmission. This involves encrypting the data during transmission using industry-standard protocols like Transport Layer Security (TLS).

Audit trails

Audit trails can provide detailed activity tracking to monitor and perform forensics in case of a security incident. The ability to capture and analyze all activities associated with a specific invoice or bill is key in ensuring ePHI is handled safely in a manner compliant with HIPAA. Audit trails are also valuable in providing assurance during internal and external audits that appropriate protocols are followed that meet HIPAA requirements.



Beyond your AP & AR automation software

HIPAA compliance for an organization goes well beyond ensuring your automated AP & AR implementation has features in place to secure and protect ePHI. For example, if you incorporate or use ePHI in any other application, you need to ensure HIPAA compliance with those application vendors as well, independently.

Each entity to which you provide ePHI, whether for storage or any other use, should have safeguards in place to protect that ePHI. For example, your AP & AR solution can enable protection for ePHI within the realm of the AP & AR application. However, if you pass or synchronize ePHI outside the application and include ePHI in your accounting system, you'll want to determine whether the accounting system software vendor offers HIPAA support.

HIPAA rules and compliance continue to evolve. Today, healthcare practices and organizations can take some key steps to help ensure their HIPAA compliance when using an AP & AR automation vendor. Seek solutions and vendors that provide protections and safeguards for the privacy and security of ePHI to help ensure that your organization remains HIPAA compliant.

For additional information on how BILL can help you with HIPAA compliance for AP & AR, please visit bill.com/industry/healthcare