SOLVE & EVOLVE

Healthcare Challenge 1 of 6: Compliance

Among other things, the HIPAA Omnibus Final Rule means vendors who handle patient information must be HIPAA compliant, too. As a provider, it's your responsibility to ensure it. So, what can you do?

CLICK

SOLVE

VERIFY VENDOR HIPAA COMPLIANCE WITH THESE 5 KEY QUESTIONS

EVOLVE

GO BEYOND COMPLIANCE WITH THESE 8 BEST PRACTICES

GET MORE IDEAS TO HELP YOU SOLVE AND EVOLVE

IRON MOUNTAIN®

SOLVE & EVOLVE IN HEALTHCARE

5 KEY QUESTIONS TO VERIFY VENDOR HIPAA COMPLIANCE

Identifying compliant vendors is tough. A little due diligence upfront can help you prevent a potentially costly privacy breach and avoid the headache of having to terminate contracts or change vendors. Ask them these basic questions:

1 HAVE YOU AUDITED YOUR SOLUTIONS TO ENSURE HIPAA COMPLIANCE?

Can they demonstrate that they have taken appropriate steps to achieve compliance?
Are policies in place to ensure continuous improvement?

2 CAN YOU DELIVER THE PROVISIONS OF OUR CONTRACT?

You should always have clear contracts with your vendors stating explicitly what your expectations are regarding the protection of patient privacy.

3 WHAT REAL PROCEDURES ARE IN PLACE TO MONITOR THE USE OF PHI?

Promises and policies are not enough. Ask your vendor for documented policies and procedures on how they will handle, track and protect PHI. Also inquire about their process for notification should there be a breach or inadvertent disclosure.

4 ARE YOUR EMPLOYEES PROPERLY TRAINED TO HANDLE PHI?

Even the best policies rely on the people who implement them. Ask your vendor to document how they hire, train and evaluate employees.

5 ARE YOUR SUBCONTRACTORS ON THE SAME PAGE?

Just as you require validation from your vendors, make sure your vendors require the same of their agents. Make sure they have signed contracts with their subcontractors that explicitly state expectations regarding the privacy and security of PHI.

IRON MOUNTAIN®

SOLVE & EVOLVE IN HEALTHCARE

8 BEST PRACTICES TO GO BEYOND COMPLIANCE

Aiming only for compliance may not fully mitigate risk. Here are a few of the numerous best practices we recommend to ensure you're taking all reasonable measures to protect patient information, remain in good standing and promote a positive image.

SECURE YOUR PHYSICAL STORAGE

Centralize your records in a secure facility equipped with physical access controls, intrusion alarms, and fire suppression systems.

SAFEGUARD PHI IN TRANSIT

Protect information in transit with advanced vehicle security features such as a dual-key ignition, driver proximity alarms, and door-ajar ignition prevention. Also, be sure to use real-time wireless scanning to maintain chain of custody.

DOCUMENT THE DESTRUCTION

Create consistent procedures and audit trails so destruction happens according to federal and state requirements – and you can prove it.

ROUTINELY SCREEN AND TRAIN YOUR PEOPLE

Handling information takes human interaction. Put a premium on proper screening, background checks, training and workflow monitoring.

PREVENT UNAUTHORIZED ACCESS

Document processes and assign role-based permissions that limit access to only the minimum necessary required for a specific job or task.

PROTECT ELECTRONIC INFORMATION

Deploy security controls for electronic data, such as encryption, authentication and passwords. Pay close attention to passwords to ensure that are unique, complex and updated frequently.

PLAN FOR DISASTERS

Don't pick a recovery and continuity plan "off the shelf." Create it specific to your operational needs and test it at least once a year.

STAY ON TOP OF BUSINESS ASSOCIATES

Be sure they are HIPAA compliant, can meet the requirements of your contract and hold their subcontractors to the same standards.

IRON MOUNTAIN®