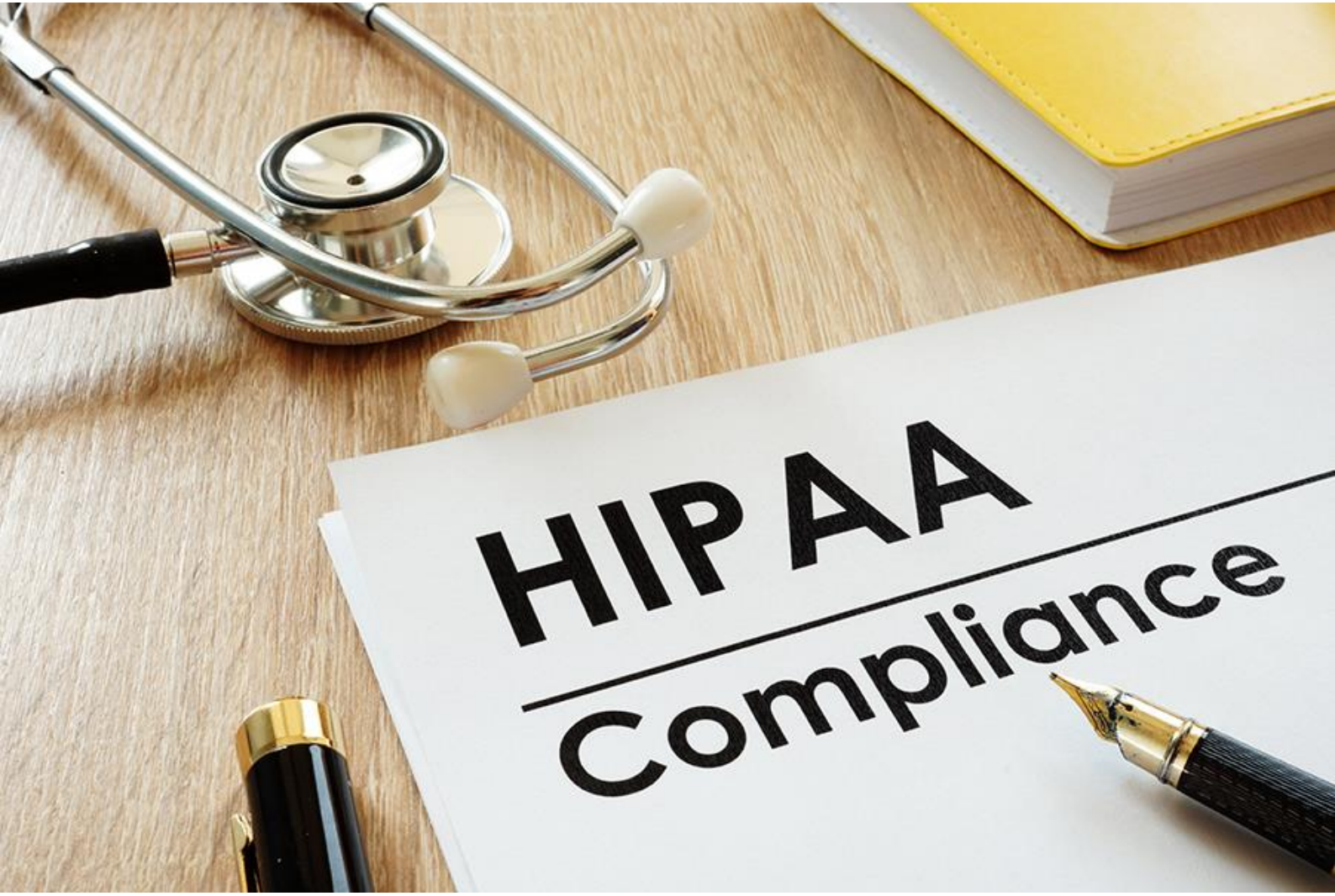

DataRails HIPAA & HITECH Compliance

What is HIPAA/HITECH?

HIPAA (the 1996 Health Insurance Portability and Accountability Act) and HITECH (the 2009 Health Information Technology for Economic and Clinical Health Act) are federal mandates that require specific security and privacy protections for Protected Health Information (PHI).

DataRails

HIPAA/HITECH Key Terms

Covered entities are healthcare providers, healthcare clearinghouses, or a health plan.
Business associates are companies that work with covered entities. Business associates may be subject to HIPAA/HITECH.
Protected Health Information (PHI) is individually identifiable medical and health-related information that relates to someone's past, present, or future. It includes:

- medical or psychological conditions
- provisions of medical service
- payments for medical service

Personally Identifiable Information (PII) is a subset of Protected Health Information (PHI). It refers to information that is uniquely identifying to a specific individual, such as name, date of birth and address.

Does DataRails facilitate HIPAA compliance for its customers?

- The DataRails product/platform meets the obligations required by HIPAA and HITECH.
- Customers are responsible for requesting the correct configuration from the DataRails customer success team for enforcing policies in their organizations to meet HIPAA compliance.

Is there any kind of industry certification that DataRails has undergone to prove it supports HIPAA compliance?

- There is no official HIPAA/HITECH certification. In order to support HIPAA compliance, DataRails has reviewed the HIPAA regulations and updated its product, policies and procedures to be HIPAA compliant.
- DataRails has also been evaluated by an independent, third-party auditor who has issued an evaluation report (HIPAA AUP) that details the controls DataRails has in place to meet HIPAA requirements in regards to data privacy and security. You may request the third-party audit report on DataRails HIPAA compliance by contacting your DataRails account executive.

How does DataRails support HIPAA compliance within its product and platform?

DataRails offers the following features:

- Data encryption
- Restricted physical access to production servers
- Strict logical system access controls
- Configurable administrative controls available so you may:
    - Grant authorization to files to read, download, edit, lock and password protect files
    - Monitor access
    - Receive an audit trail of account activities on both users and content
    - Benefit from a formally defined and tested breach notification policy
- Additional safeguards include:
    - Highly restricted employee access to customer data files
    - Mirrored, active-active data center facilities to mitigate disaster situations
    - 99.9% uptime SLA
    - SOC2 compliance
    - Training of DataRails employees on security policies and controls

DataRails also supports HIPAA compliance as follows:

Product-related features
DataRails gives you the flexibility to configure your account so fileboxes cannot be shared with people outside of your organization. You also have the option to customize the filebox settings and choose the appropriate level of access per user — edit or view-only.

Strengthen authentication SSO
DataRails has an option to perform SSO using Microsoft LIVE account, Google login and Onelogin. You may want to set up a single sign-on for DataRails by using your existing SSO provider so that your team members don't have to remember yet another password. More importantly, authenticating access to DataRails will be managed using the same password policies as other services at your company.

Unlimited version history
By default, DataRails provides unlimited version history and deletion recovery, meaning that every time a user save an Excel file(*), a new version is stored to the DataRails server, including all required metadata such as user name, date, time etc.

* requires the user to use DataRails sync services (DataRails Widget or DataRails shared folder sync service)

Access control
Team members can be easily added, removed and reviewed from the Admin Console. To ensure that sensitive data in your DataRails account can only be accessed by appropriate people, we recommend frequently reviewing this list. You can then remove access when someone leaves your organization or no longer requires access because of a change in job role.

Unusual activity monitoring
DataRails admins can view and export reports that detail your team's sharing, authentication and administrator activities. We recommend that you review these activity reports to keep an eye out for any unusual activity and help keep your team secure.

For any question, please contact support@datarails. com