HIPAA Compliance with Bigin

The Health Insurance Portability and Accountability Act (including the Privacy Rule, Security Rule, Breach notification Rule, and Health Information Technology for Economic and Clinical Health Act) ("HIPAA"), requires Covered Entities and Business Associates to take certain measures to protect health information that can identify an individual. It also provides certain rights to individuals. Zoho does not collect, use, store or maintain health information protected by HIPAA for its own purposes. However, Bigin by Zoho CRM provides certain features (as described below) to help its customers use Bigin by Zoho CRM in a HIPAA compliant manner.

HIPAA requires Covered Entities to sign a Business Associate Agreement (BAA) with its Business Associates. You can request our BAA template by sending an email to legal@zohocorp.com

HIPAA compliance in Bigin

HIPAA compliance is applicable for the Contacts module in Bigin.

When a healthcare organization starts using Bigin to store customer information in a shared database, it is crucial that they ensure the confidentiality of an individual's health information.
In Bigin, we provide ways for healthcare organizations to secure and restrict export of individuals' health information and stay compliant with HIPAA.
The Bigin admins can achieve the above by performing the following steps:

1. Marking fields that contain PHI (Personal Health Information)
In the Contacts module, there may be only a few fields that contain personal health details of a customer. For example, surgical history, symptoms, medication details, etc. marking these fields as PHI will help the system identify and restrict access to these fields through API and prevent the export of these field values. A total of 30 fields can be marked as PHI fields.

Note: Lookup and auto number fields cannot be marked as PHI.

2. Setting restrictions for the data marked as PHI
There are four options for restricting PHI from being accessed outside Bigin. Any of these options can be enabled depending on the org's requirements:

i. **Restrict data access through API**
Other applications can connect with Bigin using API and data can be transferred. You can ensure that PHI of

your customers is not shared in the process, by restricting transfer of personal health data to other applications via API.

ii. **Restrict data export**
While exporting data from the Bigin account you may want to withhold PHI from being exported by enabling this option.

iii. **Restrict data transfer to Zoho Services**
If the Bigin account is integrated with other Zoho applications like Desk, Campaigns, Books etc. the data will flow from Bigin to these applications. This option will prevent PHI from being transferred to other apps.

iv. **Restrict data transfer to third party Services**
If your Bigin account is integrated with third party applications, there will be data flow from Bigin to these apps when the records are synced between Bigin and the third party services. This option will prevent PHI from being transferred to other apps.

3. Encrypting PHI fields

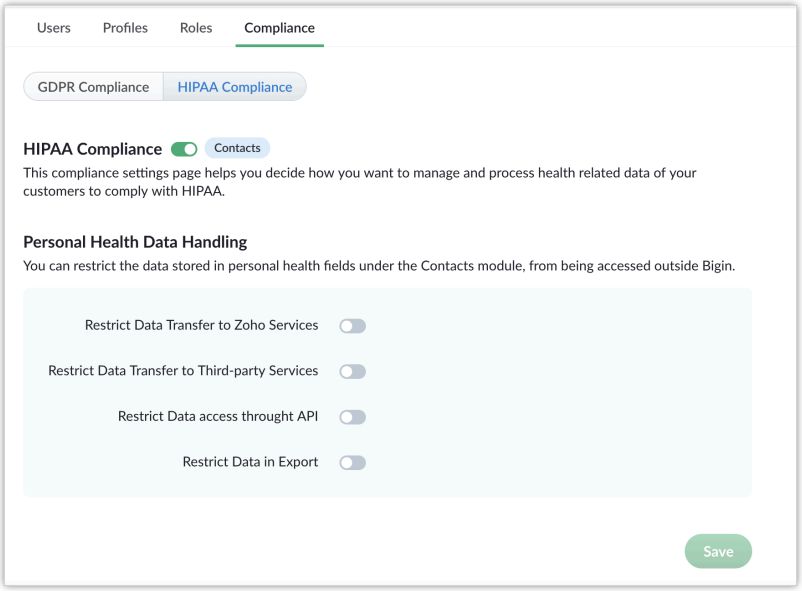
Fields that are marked as PHI can be encrypted for additional security. Though field encryption is not a mandatory step in Bigin, we strongly recommend you enable encryption as it is the best practice to prevent unauthorized access.

ⓘ Refer to the Zoho Encryption whitepaper to understand the encryption process and key management in detail.

To configure HIPAA compliance

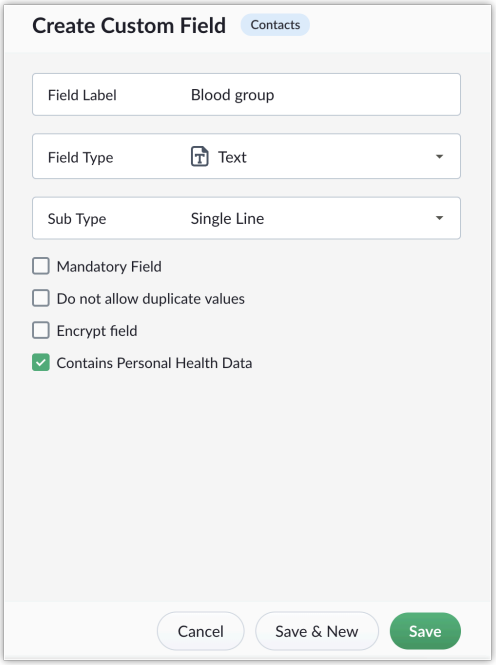
1. Go to **Settings** > **Users and Controls > Compliance.**
2. Click the **HIPAA Compliance** tab**.**
3. Enable the **HIPAA Compliance** button.
4. In *Personal Health Data Handling* section, toggle any of the following options, as required:
    a. Restrict Data access through API
    b. Restrict Data in Export
    c. Restrict Data transfer to Zoho Services

d. Restrict Data transfer to Third-party Services.



To mark fields that contain personal health data

1. Go to **Settings** > **Fields**.
2. In **Contacts** module, go to the desired field and click the **Edit** icon.
3. Check the **Contains Personal Health Data** box.
   Remember that this option will only appear if HIPAA compliance is enabled in your Bigin account.

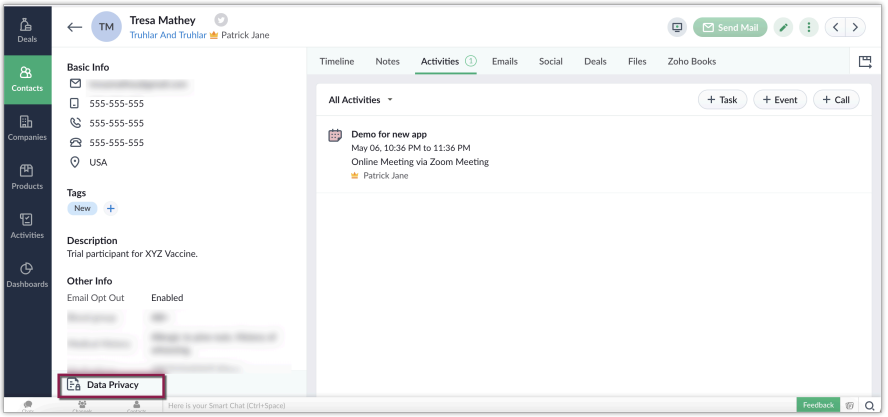


Disabling HIPAA compliance

Once HIPAA compliance is disabled, the fields that have been marked as PHI will be unmarked. The admin can mark the fields again when they re-enable the HIPAA compliance.

Viewing personal data of the records

All the fields that are marked as containing PHI will be listed in the record detail page. Under Data Privacy, in the Personal Data section, you can click the Health tab to view the fields that have PHI.



⚠ Kindly note that the content presented here is not to be construed as legal advice. Please contact your legal advisor to learn how HIPAA impacts your organization and what you need to do to comply with the HIPAA.