Red Hat HIPAA Implementation Guide

We understand the need to ensure that your organization's data is safe and secure in accordance with applicable laws and regulations. We developed this guide to help you use our products in a way that complies with the Health Insurance Portability and Accountability Act and its implementing regulations (HIPAA). This guide is intended for Red Hat customers that have a business associate agreement (BAA) in place with us, or intend to enter a BAA with us.

Background on HIPAA

HIPAA is a federal law designed to protect the privacy and security of protected health information (PHI) that is generated or maintained in the course of providing health care services.

PHI is individually identifiable health information that is transmitted by, or maintained in, electronic media or any other form or medium. This information must relate to (1) the past, present, or future physical or mental health, or condition of an individual, (2) provision of health care to an individual, or (3) payment for the provision of health care to an individual.

HIPAA applies to covered entities, including health plans, health care clearinghouses, and health care providers that transmit electronic health information in connection with certain standard transactions (e.g., billing a health plan for services), as well as to their business associates, which include third parties that perform certain functions or activities that require the use of PHI.

Business associates are vendors that perform services on behalf of, or provide certain services to a covered entity that involve the creation, receipt, maintenance, or transmission of PHI. A business associate may also include a subcontractor that creates, receives, maintains, or transmits PHI on behalf of another business associate.

Use of Red Hat Products Consistent with HIPAA

Customers are responsible for ensuring that their organizations utilize Red Hat products in a HIPAA-compliant way. Only certain Red Hat services are eligible and approved to handle PHI. For a list of HIPAA-Qualified Online Services, please refer to this list. If you plan to use Red Hat HIPAA-Qualified Online Services for handling PHI, you will need to assess whether a BAA is necessary with Red Hat and, if so, will need to review and execute Red Hat's BAA.

The BAA that customers sign with us covers only applicable Red Hat HIPAA-Qualified Online Services. Customers are responsible for configuring and using the covered services with the appropriate security controls and conducting reviews as appropriate. While using a Red Hat HIPAA-Qualified Online Service, note that we do not monitor or analyze the data that customers input within Red Hat services. We provide self-controlled security features, and we recommend that customers have the required processes and procedures in place to ensure that users adhere to end-to-end compliance

Customers are responsible for ensuring that all third party applications used in conjunction with the Red Hat HIPAA-Qualified Service are operated in a HIPAA-compliant manner. We also recommend that customers determine if they require a BAA or other privacy and security protections prior to sharing any PHI with a third party. Be aware that the Red Hat HIPAA-Qualified Online Services require you to purchase infrastructure services from a third party cloud provider. You are responsible for determining if a Business Associate Agreement is required and if applicable, signing it with the third party cloud provider, and ensuring the third party complies with HIPAA.

Configuring your Red Hat Account Consistent with HIPAA Requirements

If you will use a Red Hat HIPAA-Qualified Online Service to process or maintain PHI, follow these steps to appropriately configure your Red Hat account:

Step 1: Identify the applicable Red Hat HIPAA-Qualified Online Service(s) at https://access.redhat.com/articles/2918071;

Step 2: Determine whether a BAA is necessary with Red Hat and, if so, enter into a BAA with us.

Step 3: Implement any security measures within your account that are appropriate for your use, such as encrypting data at rest and using TLS secure endpoints, etc. While Red Hat provides options to enable a customer to secure its environment, Red Hat is not responsible for implementing those tools.

Limitations on Your Use

UNDER NO CIRCUMSTANCES SHOULD YOU ENTER ANY PHI INTO SUPPORT TICKETS RAISED WITH RED HAT EITHER DIRECTLY WITHIN THE TICKET OR WITHIN ANY LOGS, CASE COMMENTS OR OTHER ATTACHMENTS SENT TO RED HAT IN CONNECTION WITH TROUBLESHOOTING OR TECHNICAL SUPPORT. YOU SHOULD ALSO NOT PUT ANY PHI IN ANY COMMUNITY SUPPORT FORUMS, OR LOGS. PHI SHOULD NOT BE USED IN CLUSTER NAMES OR AS PART OF LOGGING.

Individual Rights Requests

To the extent Red Hat receives any requests from individuals to exercise rights afforded under HIPAA, in accordance with our BAA Red Hat shall forward such requests to you for processing. Customers have access to individual PHI in our HIPAA-Qualified Online Services in order to facilitate processing requests for access and amendment of PHI in a Designated Record Set. Red Hat will not otherwise process, handle or respond to such requests directly.

Termination of the BAA

If the BAA terminates or is terminated, you may no longer have access to the HIPAA Qualified Services. PHI should be retained in your own cloud provider account and not in any Red Hat Services.

State Law Requirements

Some state health information privacy and sensitive condition laws and other federal laws are more restrictive than HIPAA or impose additional requirements on the use and disclosure of identifiable health information. Customers are responsible for confirming that their use of Red Hat HIPAA-Qualified Online Services is consistent with applicable state and federal laws. By using the Red Hat HIPAA-Qualified Online Services for processing or maintaining identifiable health information, you are representing that: (1) such use, and your disclosure of information to Red Hat through the services, complies with applicable state and federal laws; and (2) you have obtained all necessary consents, authorizations and permissions required by applicable law to share information with Red Hat in connection with Red Hat's HIPAA-Qualified Online Services.

Disclaimer

This HIPAA implementation guide is for informational purposes only. Red Hat does not intend for the information in this guide to constitute legal advice. You should evaluate your particular use of Red Hat's products as appropriate to support your compliance obligations in accordance with applicable law. We may update or revise this guide from time to time, you can subscribe to this page to receive updated versions.