Adamo Diagnostics, LLC

Shared Responsibility Policy

Last Updated: January 19, 2022

Since Add Your Labs's LIMS is highly configurable and cloud-based, there may sometimes be uncertainty regarding security responsibilities. The text below clarifies what Add Your Labs is responsible for and what you, the customer, are responsible for.

Please feel free to submit any questions about this Shared Responsibility Model in particular, or Add Your Labs security in general, to support@AddYourLabs.io.

Summary concept

Add Your Labs is responsible for the security of the capabilities offered and of the supporting infrastructure, whereas you are responsible for how those capabilities are configured and how your workforce and third parties use them.

You may sometimes enlist Add Your Labs, as your agent, to configure Add Your Labs for you. (For some kinds of configurations, Add Your Labs's assistance is required; for others, you have the option to do the work yourself.) Regardless of who implements the configuration, you are responsible for the security implications.

HIPAA and the Business Associate Agreement

You, our customer, are a Covered Entity and we are your Business Associate, per HIPAA's definitions of those terms. We executed a Business Associate Agreement with you when your subscription began. That agreement established our respective obligations and supersedes the text below, which is meant only to add details to those obligations (not replace or amend them in any way).

We sometimes engage subcontractors to deliver the service to you. In those cases, the subcontractor will have access to your protected data. We execute a Business Associate Agreement with our subcontractors that is substantially similar to the one we execute with you. In this way, specified security obligations are passed to contractors and remain in force under HIPAA.

Access Control

When you start your Add Your Labs subscription, Add Your Labs creates an "organization" which segregates you from other Add Your Labs customers. All access is controlled within this organization.

Your obligations with respect to account administration and control are covered in the Terms of Service. As described there, we create initial user accounts with full access for the people you specify. From that point forward, you are responsible for these accounts and for creating whatever additional accounts you may need (which you can do, using documented features, with these full-access accounts). This responsibility includes both who is allowed to access your organization but also what they are allowed to do within your organization.

Add Your Labs provides a flexible, role-based model that controls what can be done under an account. You are responsible for configuring and granting these roles according to your policies, which should include the "principle of least privilege." If you choose to use the default roles as configured by Add Your

Labs, then you are still responsible for understanding those roles and granting them appropriately. Please review the documentation regarding permissions and configuring and granting roles to accounts.

Your access control responsibility extends to programmatic access, including integrations between Add Your Labs and third party systems with which you have a direct relationship. You should familiarize yourself with the mechanisms for these, such as Add Your Labs API keys and SFTP account configuration, and institute systems to track and maintain this access just as you should for interactive access.

If you choose to allow providers to access Add Your Labs's portal, you are responsible for whether that is done according to your policies and your arrangement with those providers.

Add Your Labs is responsible for enforcing access according to its documented capabilities. This includes both enforcing authentication (who is allowed access) and enforcing permissions (what they are then allowed to do) as documented.

Add Your Labs is also responsible for access to the service and the underlying infrastructure that we confer to our own workforce and to third parties engaged directly by us. This includes rigorous controls, including routine evaluation of the controls implemented by third parties, and frequent reviews to confirm compliance and least-privilege.

Integration with Third Parties

You may sometimes take advantage of integrations with third parties that send your protected data to them or allow them to view or modify your protected data in Add Your Labs. This is usually system-to-system integration (through code, provided either by Add Your Labs or by the third party). But it is access to data nevertheless and can be a security risk if not managed properly.

Sometimes Add Your Labs engages directly with a third party to provide you with an advertised capability. In these cases, that third party is Add Your Labs's subcontractor, has executed a Business Associate Agreement and is subject to Add Your Labs's rigorous vendor management policies and procedures. In these cases, Add Your Labs is responsible for the access granted to that third party on your behalf.

More commonly, you directly engage a third party in a Business Associate Agreement to take advantage of an integration built and supported either by Add Your Labs or that third party. In these cases, you are responsible for the access you grant to that third party.

We recommend that you track and frequently review such access and periodically rotate passwords or API keys, depending on the details of that integration.

Control of Artifacts

You are responsible for artifacts that you direct us to deliver from the system. This of course includes downloaded files, screenshots and other artifacts delivered directly. It also includes faxes you have directed us, per the configuration, to send. Add Your Labs is responsible for sending them to the number you configured; you are responsible for confirming the correct fax number.

Note that you can configure Add Your Labs to send emails regarding patient results but that these emails themselves do not include patient data (but rather give a link to access it). However, they do include the requisition identifier, so you should not embed patient data in requisition identifiers.

Use of Support Services

We are both obligated not to share PHI outside of the Add Your Labs service. We will not directly send PHI to you and you should not send it directly to us. Add Your Labs offers a facility to safely exchange PHI within our product, the details of which are available from support@AddYourLabs.io.

In the rare case that you are sometimes granted access to other Add Your Labs systems, do not put PHI in those systems either.

If we notice PHI in our support system (or any other system outside of our production service), we will remove it, but we do not guarantee that we will do this in a timely fashion nor have control over, nor be able to report on, who in our workforce will have had temporary access to it.

Security Incidents

You must notify us at support@AddYourLabs.io if you become aware that a user account in your organization was accessed by an unauthorized individual.

You can also notify us in the same way regarding a suspected breach or any other security concern.

As required by 45 CFR §164.410 and specified in our Business Associate Agreement, we will notify you of any breach of unsecured PHI no more than 10 days after we discover it.

Platform Security

Add Your Labs is responsible for applying best practices for a secure cloud service. These include encryption, routine vulnerability scans, active detection of security events, and more. We are happy to share more information about these practices. Just reach out to support@AddYourLabs.io.