Updox Partner Portal Acceptable Use Policy (AUP)

Effective August 4, 2025

Access to the Updox Partner Portal ("Portal") is conditioned upon your acceptance of this Acceptable Use Policy ("AUP"). By clicking to accept, you acknowledge that you have read, understood, and agree to comply with its terms.

This AUP may be updated from time to time at Updox's discretion. The most current version will be available at https://help.updox.com/help/partner-portal-acceptable-use-policy. Your continued use of the Portal after any update constitutes your acceptance of the revised AUP.

1. Purpose and Scope

This Acceptable Use Policy ("AUP") governs your access to and use of the Updox Partner Portal (the "Portal"). The Portal allows authorized users of Updox partners ("you," "your," or "User") to create and manage Updox customer accounts, manage vendor-level integrations and forms, and perform related administrative functions under your partner organization's ID.

The following terms supplement any and all agreements between Users and Updox and apply to your use of and access to the Updox Partner Portal and any associated or connected systems.

This AUP applies to all individual users, regardless of role (Admin, Manager, Basic), and is binding on all users each time they log in to the Partner Portal.

2. Acceptable Use Requirements

You agree to use the Portal solely for legitimate business purposes in accordance with applicable law, including but not limited to the Health Insurance Portability and Accountability Act ("HIPAA"). You are responsible for any transmission you send, receive, post, access, or store via the Portal, including the content of any communications. This includes but is not limited to your agreement to:

- Maintain the confidentiality of your login credentials and enable MFA as required.
- Take full responsibility for all activity generated by your assigned User account with the understanding that you are prohibited from sharing your credentials under any circumstance.
- Access only those customer or partner resources that you are authorized to manage.
- Be solely responsible for all activity, permissions, and authorizations required by third-party services you configure, enable, or otherwise utilize via the Portal or an integration with the Portal.

3. Prohibited Conduct

Transmitting, distributing, or storing any material that violates any applicable law is prohibited, as is any use that may compromise the security, confidentiality, or integrity of the Portal, customer data, patient data (PHI/ePHI), and/or any Updox system or third-party system connected to or integrated with the Portal. Prohibited conduct includes, without limitation, the following actions:

- Disabling or otherwise circumventing MFA for your User account or any other User account you manage.

- Exporting, downloading, or transferring data in a manner inconsistent with your business-necessary use or this AUP (“Improper Data Export”), including exporting any customer data for unauthorized personal use, resale, or third-party processing outside permitted integrations.
- Uploading any electronic protected health information (ePHI) or personally identifiable information (PII) into any non-production or testing environments within the Portal.
- Using the Portal to develop, reverse engineer, or compete with Updox services or infrastructure.
- Using the Portal or third-party services integrated with the Portal to transmit any material that, intentionally or unintentionally, violates any applicable local, state, national or international law, or any rules or regulations there under.
- Offering or disseminating fraudulent goods, services, schemes, promotions or similar fraudulent activities via the Portal or any third-party services integrated with the Portal..
- Infringement of intellectual property rights or other proprietary rights including, without limitation, material protected by copyright, trademark, patent, trade secret or other intellectual property right.
- Disseminating or posting material that is unlawful, libelous, defamatory, obscene, indecent, lewd, harassing, threatening, harmful, invasive of privacy or publicity rights, abusive, inflammatory or otherwise objectionable as determined by Updox.
- Violating the rules, regulations, or policies that apply to any third-party network, server, computer database, or website that you access via an integration with the Portal.
- Disseminating or uploading harmful content including, without limitation, viruses, Trojan horses, worms, time bombs, zombies, cancelbots or any other computer programming routines that may damage, interfere with, secretly intercept or seize any system, program, data or personal information.
- Attempting to utilize the Portal or any Updox or third party integration with the Portal to impersonate any person, company, or other entity.
- Using the Portal to access, or to attempt to access, the accounts of others, or to penetrate, or attempt to penetrate, security measures of Updox or another entity’s computer software or hardware, electronic communications system, or telecommunications system, whether or not the intrusion results in the corruption or loss of data.
- Providing a Portal Username and/or Password to anyone other than the officially registered owner of said Username and Password and/or accessing the Portal using a password not specifically issued to you.
- Using the Services to collect, or attempt to collect, personal information, including Protected Health Information (PHI) about third parties without their knowledge or consent.
- Using the Portal for any activity which adversely affects the ability of other people or systems to use the Portal. This includes “denial of service” (DoS) attacks against another Portal organization or individual user.
- Using the Portal in a manner that exposes or may expose Updox, its customers, partners, or vendors, or any other person or entity using the Portal to abuse, complaints, retaliation, connectivity issues, or other negative impact.

4. Role-Based Responsibilities

Admin Users are solely responsible for managing Manager and Basic Users within their partner organization’s portal environment, including onboarding, role assignment, deactivation, and MFA resets. Admin Users are further solely responsible for ensuring that any person to whom they issue a Portal User account is properly authorized to access any and all systems and data available to them via the Portal. Additionally, Admin Users are responsible for ensuring that all users under their management comply with this AUP, and must immediately terminate access for any User who violates this AUP or whose account may have been compromised or misused.

Manager and Basic Users must use the Portal within the access privileges granted by their role and in compliance with this AUP, and must immediately report any suspected misuse or compromise of their credentials to their organization’s Portal Admin User(s).

5. Violations and Enforcement

Any violation of this AUP may result in immediate suspension or termination of a User account by Updox or by a Partner Organization’s Admin User. Updox may, in its sole discretion, terminate any or all Users (regardless of role) within a Partner Organization based on Updox’s determination that an AUP violation by one or more Portal Users under that Organization has occurred.

Updox may involve or cooperate with law enforcement authorities if criminal activity is suspected, or with the US Department of Health and Human Services Office of Civil Rights if HIPAA violations are suspected. In addition, Users who violate this AUP may be subject to civil or criminal liability. Updox shall not be liable for any damages suffered by any User or third party resulting directly or indirectly from use of the Portal.