What are my MFA Options

ACCURO® Electronic Medical Records

		Type of device needed	Pros	Cons	Cost	When to use which
SMARTPHONE - TIME BASED ONE TIME PASSWORD "TOTP" OPTIONS						
Users will download the application of their choice. When prompted for MFA, within the app, a code will be generated to verify their log in. A smartphone is required to set up the **Accuro ONE ID** with these MFA options and access to a smartphone will be required when logging in from a new device or when needing to validate MFA.	**Okta Verify*** *Recommended*	Smartphone	- Easy setup - Easy-to-use push notifications - No additional hardware required	- Most rely on a mobile device for set up - User must select, install, and set up an additional application of their choice - To carry out MFA, user has to open that app and input a one-time passcode when prompted	FREE	The organization has no bias towards a certain product and each Accuro user has their own smartphone on which they can install the app.
	Google Authenticator	Smartphone	- Easy setup - User can configure with an application they're already using - Depending on the application, MFA can done via mobile, computer, or both		FREE	The organization may already be using one of these tools or have a preference. Accuro users with these tools will need access to smartphones.
	Microsoft Authenticator	Smartphone			FREE	
	Authy	Smartphone OR computer app			FREE, paid option available	
	1Password	Smartphone AND computer app			FREE, paid option available	The organization is in the market for a password manager and likes having the option to install it on a PC as well as access it in a browser. There may be a cost associated directly with 1Password based on the size of clinic.
BIOMETRIC OR SECURITY KEY - FAST IDENTITY ONLINE "FIDO2" OPTIONS						
FIDO Stands for Fast Identity Online it is a standard that allows trusted devices other than smartphones to provide a validation of identity. Biometric sensors may already be in use by your organization such as Yubi Key, Google Titan, Windows Hello, Apple Touch ID	**Yubi Key**	Yubi Key	- Doesn't require a mobile device - Can be used with existing tools like fingerprint reader or Windows Hello facial recognition	- Device must be set up and configured for MFA - User must choose a solution that will work in all the places they log in (e.g. a yubikey requires a specific, compatible USB port) - Yubikeys and other dedicated devices have an additional cost per user - If a dedicated device is lost, there is a cost to replace it	$50+	Individuals at the organization do not have their own smartphones and the organization is open to buying and using an external device for their MFA option. Downside: If a user forgets their YubiKey at home or its lost they would be locked out and need to have their MFA reset by QHR.
	Google Titan	Google Titan			$40+	
	Windows Hello	Built-In Sensor			Feature of PCs with Windows 10 or 11	Users with this organization are always using the same workstation. This is most convenient when these tools are pre-installed in modern devices.
	Apple Touch ID	Built-In Sensor			Feature of some Mac computers	