

# Auxita Platform: We Take Data Security Seriously



As a modern healthcare provider, you know that digital security and patient confidentiality are one and the same. A lot of patient data lives on your clinic computers; We understand that protecting that data is a critical concern for any modern medical practice.

Before connecting, you need to be completely sure that software is secure. That's why we won't just tell you Auxita is safe - our goal is to prove it. This document will show you exactly how we created, tested, and verified the security of our software so that you can feel safe using it in your practice...

## DEVELOPING A SECURE SOFTWARE & ORGANIZATION

Your privacy and security were always at the forefront of our minds. That's why we invested in a renowned, third-party security consultancy early in the development stages of Auxita.

Together with the consultancy, we underwent multiple risk management and security testing evaluations, such as:

- Subjecting our entire company to a third-party Threat and Risk Assessment (TRA);
- Completing a Privacy Impact Assessment (PIA) based on ISO standard ISO/IEC 29134;
- Creating critical base policies and procedures;
- Reviewing our early-stage platform and application for technical security risks.

**We were relentless** in implementing any recommendations that came from these evaluations. We redesigned parts of our platform to be more secure. We added more layers of protection to prevent attacks. We checked and double-checked data encryption, modifying our techniques to align with the latest privacy technology. Most importantly, we implemented checks and balances to ensure security was always prioritized in the future. **We continue to be dedicated to making every improvement, however small, that may improve your security and privacy.**

As part of this process, we subjected our systems to a formal test known as a penetration test where security experts attempted to compromise the platform. We used the results to improve our code and application workflow and then retested, greatly reducing the risk of attacks.

## TESTING, TESTING, AND TESTING SOME MORE

Every time Auxita builds a new feature to improve your experience, our developers are required to take additional privacy and security measures. For example, we developed highly secure systems to de-identify health metadata - divorcing the numbers from the identity of patients in order to track overall trends and provide valuable decision metrics. By using encryption and privacy best practices in this development, this de-identification allows you to access valuable decision metrics while strongly upholding your patients' privacy rights.

We are always evaluating our platform technology, operational measures, and security posture against the latest technology trends and best practices. This isn't just something we did at the beginning - it is something that is part of our culture. Staying one step ahead of cybersecurity threats is always a priority.

**So, go ahead and join Auxita - our security team, third-party experts, and rigorous tests have your back.**

---

*Public - No Restrictions on Distribution*

---