LOCKING DOWN CYBER RISKS: THE TRUSTED SHIELD OF SENTINAT® 200 AND FASTFINDER

IMPORTANCE OF SECURITY IN MOLECULAR DIAGNOSTICS REMOTELY

In a molecular testing setting, labs are dealing with confidential research or healthcare related data. Data security matters highly both in a clinical research setting, where research results and intellectual property need protection, and for a diagnostic solution, where labs deal with sensitive patient data, consent, and specific rules and regulations that apply to health data.

Sentinel Diagnostics developed the compact, sample-to-results system **SENTiNAT® 200** for the detection and quantification of pathogens in human samples where data security is a priority. For this reason, the **SENTiNAT® 200** is equipped with Velsera's FastFinder software, to allow the management and interpretation of data in complete safety.

FASTFINDER IS SECURE FROM THE GROUND UP

In this brief overview, we'll discuss how the FastFinder platform was built with state-of-the-art security in mind. Built from the ground up for clinical use, FastFinder provides:

- A sound and proven security model with multiple layers of security
- Regular audits and security checks
- Implementation of industry guidelines and best practices
- Partnership with a best-of-class infrastructure provider
- Audit trails and change validation

For a more detailed discussion on FastFinder's secure platform, please consult the White Paper on FastFinder's Hosted Solutions.

MULTIPLE LAYERS OF SECURITY

The FastFinder software maintains three layers of security, ensuring industry-grade security across the platform. All communication between the different modules of the FastFinder system is encrypted through TLS1.2+[1] as a security layer, combined with the OAuth[2] protocol as an authentication layer. On top of those, both the end-user facing applications and the centralized administration module provide an extra authorization layer, which allows specific user actions to be assigned to specific users through user roles.

Additionally, all data storage has been configured to be encrypted at rest, thanks to features provided by Microsoft. The underlying database storage is encrypted in the same way and benefits from the same encryption at rest as the file storage.

EXTERNALLY AUDITED PROCEDURES AND INFRASTRUCTURE

Velsera has documented procedures in place that govern its development and production infrastructure, its hosting and deployment process, its security management including user access and entitlement management, intrusion detection, and more. Moreover, Velsera regularly tasks an independent, external party to perform a full set of manual & automated penetration tests on the FastFinder software solution.

IMPLEMENTING RELEVANT SECURITY GUIDELINES

Specific rules, guidelines and best practices apply to PHI (Protected Health Information) and other health data. Velsera ensures that its platform supports compliance with guidelines such as GDPR[3], APP[4], HIPAA[5], and general industry best practices. Moreover, to ensure the highest security standards, FastFinder also allows labs to be compliant with the CAP[6] /CLIA[7] security guidelines, and uses Microsoft as a best-in-class, top notch hosting professional partner. In selecting a partner for hosting the FastFinder Platform, Velsera has chosen Microsoft Azure, a PaaS (Platform as a Service) provider that's highly secure by design, and that has a track record of providing services to software companies that manage and process PHI.

For example, Microsoft has a long history of developing highly secure & safe software for enterprises and the medical device industry that allow customers to be HIPAA[5] compliant.

For a full list of their compliance & quality efforts, navigate to the Microsoft Azure trust center, at https://www.microsoft.com/en-us/trustcenter/cloudservices/azure.

AUDIT TRAILS, CHANGE DOCUMENTATION, AND ROBUST AUTHENTICATION AND AUTHORIZATION

The FastFinder platform is built with a user-centric authentication and authorization model, which enables features like role-based access control and audit trailing. For example, whenever a user overrides an assay result in the software through the "Resolve" function, she/he is required to enter a rationale, which is stored in the audit trail for future reference.

CFR 21 Part 11, a set of regulations put in place by the United States Food and Drug Administration, describes the controls it requires to be in place to make sure electronic data is subject to signed document audit trails, record keeping, and access controls.

CONCLUSION

Velsera and Sentinel Diagnostics consider their platform security a top priority. With a sound architecture design, a secure environment, reliable partners and the right safeguards and procedures in place, you can rest assured your data are protected.

1. Transport Layer Security (TLS): Provides encryption security between client and system.
2. OAuth 2.0 is the industry-standard protocol for authorization. Provides industry standard authentication layer between client and system. See https://oauth.net/2/ for more information.
3. The General Data Protection Regulation (GDPR) is a European piece of legislation which covers personal information and how consumers and businesses interact with it.
4. The Australian Privacy Principles (APP) are part of the Privacy Act law that governs privacy of data in Australia.
5. The Health Insurance Portability And Accountability Act (HIPAA) is a USA piece of legislation which provides security provisions and data privacy, in order to keep patients' medical information safe.
6. The College of American Pathologists (CAP) is the leading organization of board-certified pathologists, and can grant accreditation to laboratories that meet a certain set of standards.
7. The Clinical Laboratory Improvement Amendments (CLIA) are United States federal regulatory standards that apply to all clinical laboratory testing performed on humans in the United States, except clinical trials and basic research.