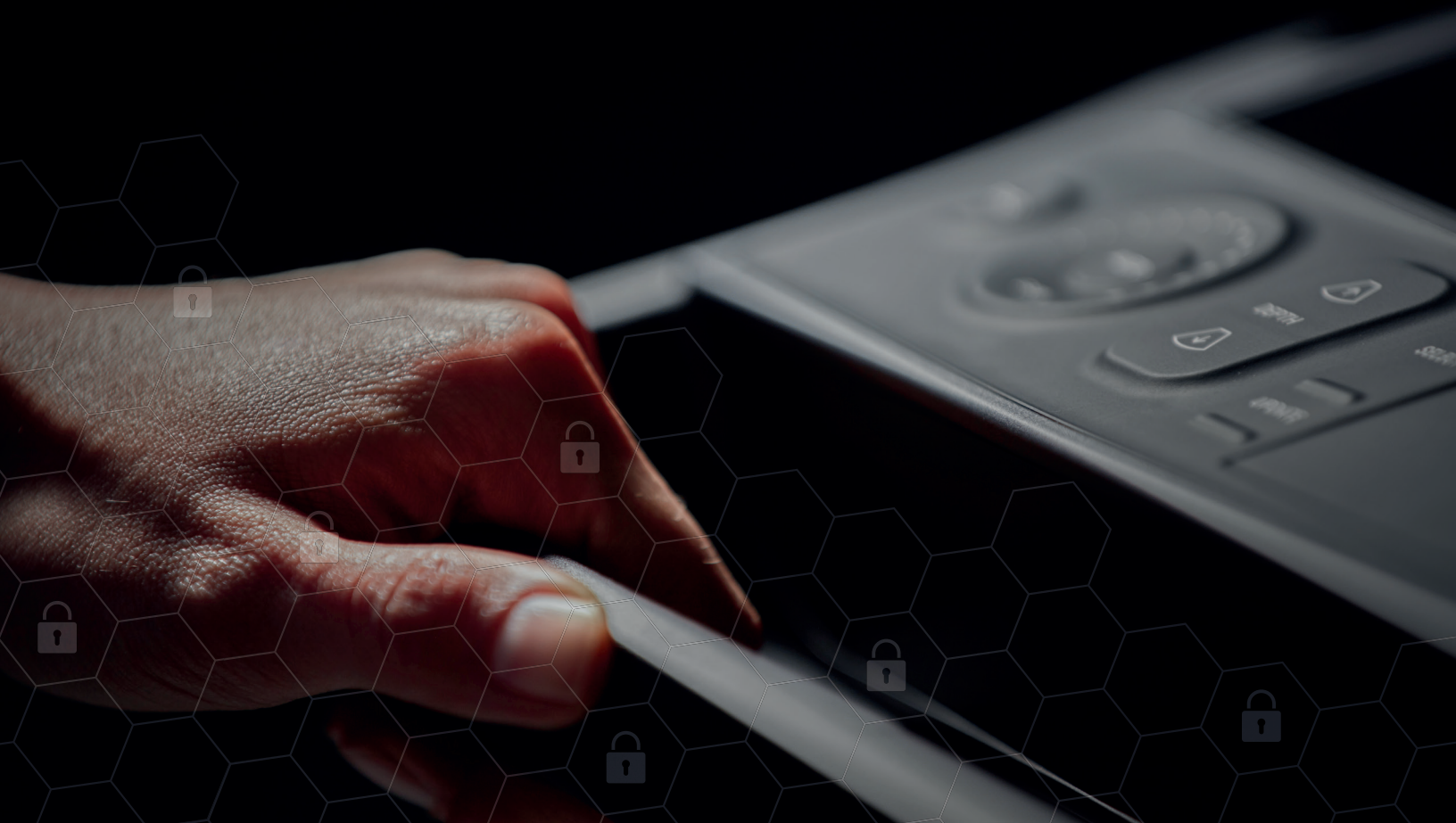
FUJIFILM
Value from Innovation

SONOSITE PX

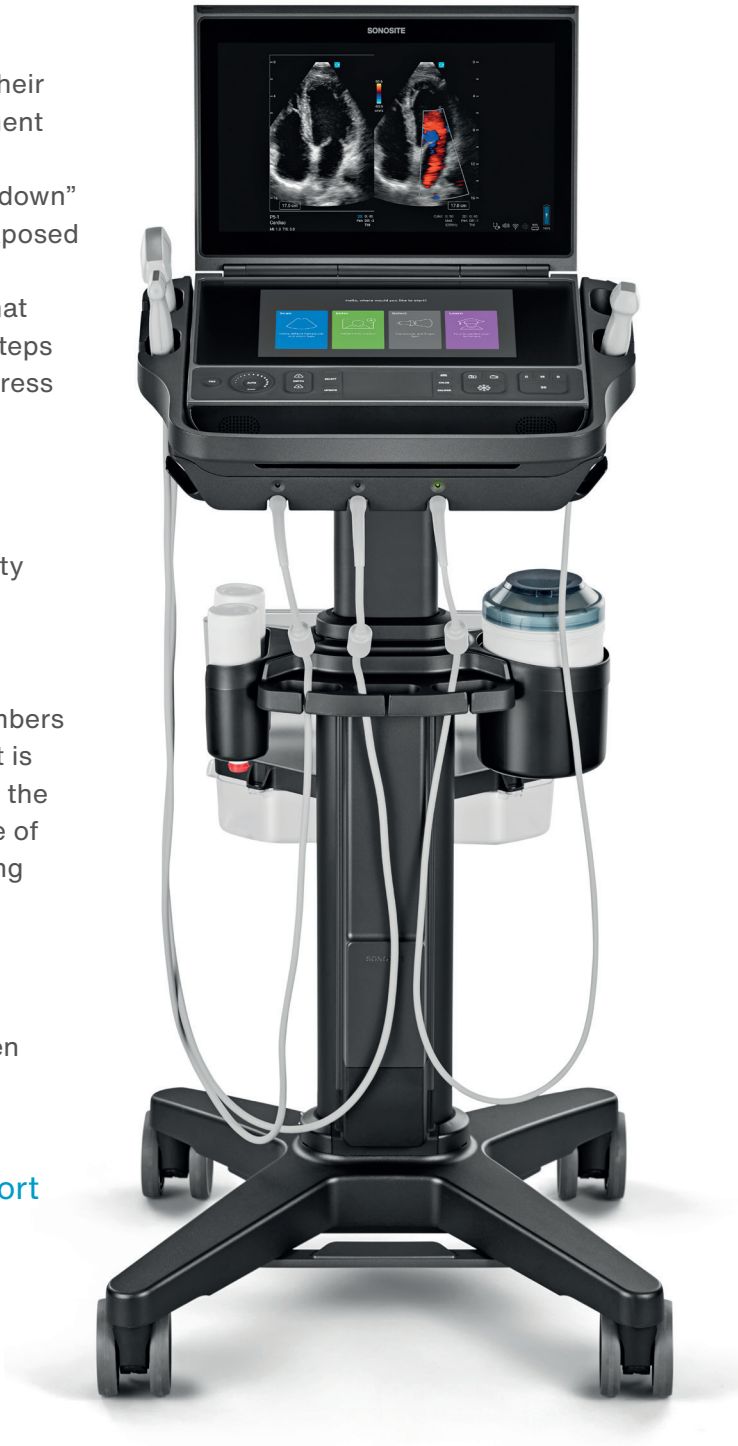
System **Security**



Sonosite Ultrasound Security

Fujifilm Sonosite understands security and privacy are a major concern for healthcare providers. We are focused on providing protection from potential security and privacy issues for our point-of-care ultrasound solutions. Through industry best practices, Sonosite ensures the security and privacy of its devices as well as the integrity of patients' Protected Health Information (PHI). Our systems are designed and engineered in-house with security and privacy in mind. Post market, we actively monitor for potential cyber security issues that may affect the devices we manufacture. We work with industry peers and partners to share cyber security information to help the community quickly react to cyber threats.

Sonosite is committed to designing point-of-care ultrasound solutions that meet the security needs of our customers and their patients. During product development, our Security Development Lifecycle (SDL) process helps us to understand and mitigate security risks before they occur. Sonosite intentionally "locks down" our ultrasound software to ensure that our devices are less exposed to security vulnerabilities. Once a system is available to our customers, we continually monitor for cyber security issues that may affect our systems. If an issue is identified, remediation steps are taken and a software update will be made available to address the issue.



Sonosite PX Security Features

Sonosite PX ultrasound systems include a robust set of security features to keep your patient information safe.

Secure Boot

Secure boot is a security standard developed by industry members to help make sure that a device boots using only software that is trusted by the Original Equipment Manufacturer (OEM). When the device starts, the firmware checks the signature of each piece of boot software, firmware drivers, applications, and the operating system. If the signatures are valid, the system boots, and the firmware gives control to the operating system.

User and Role-Based Authentication

Sonosite PX supports user and role-based authentication when configured in secure mode. This enables you to manage your users in groups such as clinicians and administrators.

Lightweight Directory Access Protocol (LDAP) Support

To be more efficient, many healthcare organizations perform their user management and maintenance in one central place. Sonosite PX uses LDAP to make user management and maintenance simpler for your healthcare organization.

Protection Starts with a Password

Sonosite PX comes with the tools required to enforce complex passwords, minimum password length, automatic password aging, and password history re-use limit rules. Sonosite PX meets the stringent Federal Information Processing Standards for moderate security control selections per FIPS199, FIPS200, and NIST 800-53.

Federal System Use Notification Support

Sonosite PX supports the Federal System Use Notification Banner as required by any U.S. federal government agency. While this functionality has a specific purpose for the U.S. federal government, Sonosite PX can be used by civilian healthcare organizations to communicate messages or special procedures to the users of the device. This feature is customizable by your system administrator.

In **2019**, more than **35 million** people are known to have had their healthcare records compromised, exposed, or impermissibly disclosed.[1]

Emergency Access

Emergency Access mode allows a clinical user to perform life-critical exams and procedures even in the event where the hospital infrastructure might be available, but there isn't time to access it.

Secure DICOM Communication Support

Sonosite PX devices support Standard and Secure DICOM transfer, ensuring patient privacy, confidentiality, and integrity. Secure data communications are further provided by using industry standard Transport Layer Security (TLS) 1.2.

Keep Your Stored Data Safe

Sonosite PX helps mitigate data loss by encrypting all data on the patient drive.

Protect Data You're Transferring

As a portable device, your device data transfers are mostly accomplished wirelessly. Sonosite PX can be configured with FIPS 140-2 validated encryption algorithms that encrypt data during wireless and wired communications, protecting your patient information.

White-Listing to Protect Your System from Unauthorized Applications

Sonosite PX comes with state-of-the art white-listing which allows only manufacturer-approved applications to function or execute. Sonosite PX does not allow clinical users or administrators to install applications. Only Sonosite PX updates can be installed on the device by an administrator.

Hardened to STIGs Standards

Sonosite PX has been hardened using U.S. Department of Defense STIGs (Security Technical Implementation Guides) to minimize outside threats. In addition, only services and applications used for clinical application are included on the system.

A Troubling Trend

Within the first six months of 2019, almost three times the number of security breaches were reported as compared to 2018. In May 2019, a record-breaking 46 breaches of more than 500 medical records were reported to the Department of Health and Human Services' Office for Civil Rights. Only two months later, another 50 incidents of security breaches were reported. More healthcare records were breached in 2019 than all of 2016, 2017, and 2018 combined.[1]

Further Information

For more information about Sonosite security, please visit the Security page on our website or contact your Fujifilm Sonosite representative.

MDS2

The Manufacturer Disclosure Statement for Medical Device Security (MDS2) provides us a way to communicate with you in a standardized language for security. A form for each of our products, outlining their security-related features can be found on our website, or from your Fujifilm Sonosite representative.

Cyber Security Notifications

Our security team is constantly working to keep Sonosite devices secure from the most recent threats. Whenever a new cyber security vulnerability is identified, we'll keep you informed of any potential impact to Sonosite systems through updates on our website.

[1] July 2019 Healthcare Data Breach Report. HIPPA Journal. https://www.hipaajournal.com/july-2019-healthcare-data-breach-report. Published August 29, 2019.

FUJIFILM Sonosite, Inc.
21919 30th Drive SE
Bothell, Washington 98021-3904
United States
Tel: +1 425 951-1200
Fax: +1 425 951-1201
www.sonosite.com

FUJIFILM Value from Innovation SONOSITE

Any patient. Anywhere. Anytime.

MKT03454 Rev A 6/2020