FORTRA

DATASHEET (GoAnywhere)

Meeting European Compliance Requirements for Healthcare

As healthcare organizations rapidly adopt health information technology like EHR software, unsecure file transfer methods (e.g., use of legacy tools and homegrown scripts) are creating risks that leave healthcare providers open to vulnerabilities and data breaches. It's critical for European organizations to secure their data and update their business processes to ensure they meet local, national, and EU-wide compliance requirements.

GoAnywhere Managed File Transfer (MFT) gives healthcare organizations a safe, streamlined way to send files and sensitive ePHI and EHR data to hospitals, clinics, pharmacies, and insurance companies. It can help organizations meet critical compliance standards while saving time and money in other business areas. It can also eliminate the custom programs and scripts organizations normally use to transfer data, improve the quality of file transfers, and provide tight administrative control and audit reports for heightened security measures.

Address Your Security and Compliance Needs

GoAnywhere MFT helps healthcare organizations meet European compliance requirements like the GDPR (General Data Protection Regulation) by providing an auditable solution with secure file transfers, data encryption, and audit logging. The benefits of GoAnywhere for security and compliance needs include:

KEY GDPR REQUIREMENTS FOR HEALTHCARE ORGANIZATIONS

Healthcare organizations in Europe have a lot to consider when ensuring total data security compliance with local, national, and EU-wide regulations. The GDPR is no exception. Health providers need to ensure they're aligned with the following key concepts of GDPR:

- Informed consent must be given by subjects involved
- Existence of a DPO (Data Protection Officer)
- Pseudonymization vs. anonymization
- Right to forget, portability, and access
- Rules for transferring data outside the EU

GoAnywhere MFT can help achieve GDPR compliance for your file transfers. See the next page for a list of which required standards GoAnywhere is able to address.

Control of Sensitive Patient Data
GoAnywhere's centralized controls, security settings, support for popular transmission protocols, and ease-of-use help authorized users transfer PHI data with confidence.

Auditing of File Movements & Activity
GoAnywhere automatically records and retains logins, file transfer transactions, and encountered errors. These audit logs and reports satisfy compliance regulations that require documentation of where ePHI data is transmitted.

File Encryption & Secure File Transfers
GoAnywhere's centralized controls, security settings, support for popular transmission protocols, and ease-of-use help authorized users transfer PHI data with confidence.

Enhanced Reverse Proxy
GoAnywhere Gateway is an enhanced reverse and forward proxy solution that provides extra security for data exchanged with trading partners and vendors. It ensures file sharing services and documents are kept safely in an organization's internal network and out of the DMZ (Demilitarized Zone).

Reduced Costs & Streamlined Processes
GoAnywhere's automated workflows and transaction alerts allow healthcare IT staff to streamline mundane tasks, automate business processes, and spend more time on other important projects.

Case Studies

GoAnywhere MFT gives healthcare organizations a safe, streamlined way to meet compliance requirements and send sensitive ePHI and EHR data to hospitals, clinics, pharmacies, and insurance companies. Explore these case studies to see examples of how real health providers across the globe use GoAnywhere to achieve their critical business initiatives.

Protect Your PHI and ePHI Data with Encryption

European data security standards often require the personal data of EU citizens to be secured. Organizations must be able to provide a reasonable level of data and file transfer security, no matter if the data is located on-premises, remotely, or in the cloud.

In order to comply with these requirements, companies should implement encryption as part of their security policies. GoAnywhere MFT offers several popular technologies to help businesses secure sensitive data at rest and in transit. Use OpenPGP, SSL, SSH, ZIP with AES, and more to ensure your business and clients are always protected.

Cancer Registry of Greater California

Benefit: Boosted team collaboration and productivity.

When the Cancer Registry of Greater California realized they needed a simple, secure way to exchange confidential patient data with their trading partners, they migrated from their old file transfer processes (20-25 secure email subscriptions) to GoAnywhere MFT, a solution that met their long list of security, file transfer, and collaboration requirements.

Learn More

CRGC
CANCER REGISTRY OF GREATER CALIFORNIA

Nemours Children's Health System

Benefit: Major time savings and improved file transfer security.

Nemours Children's Health System cares for over 300,000 children annually. Upon looking for a versatile and reliable system that could handle a high volume of file transfers (5,000+ a month), GoAnywhere MFT fit the bill. The new solution helped them maintain critical security standards, reduce the time spent on implementing projects, and troubleshoot transfer errors.

Learn More

Nemours.
Children's Health System

AnMed Health

Benefit: Reduced staffing resources and achieved file transfer stability.

When AnMed Health recognized their current FTP processes for file transfers were inefficient and unsecure, they set out to find a replacement that was easy to learn, supported job auditing and troubleshooting, and included system notifications. GoAnywhere MFT was all this and more, and saved AnMed Health over 500 hours of staff work a month.

Learn More

ANMED HEALTH

GDPR Compliance Table

For many organizations, the GDPR is the most pressing compliance standard to address. GoAnywhere MFT can help healthcare providers address GDPR requirements through several key features, including data encryption, integrity checks of successful file transfers, secure forms for subject consent, and detailed audit trails.

GDPR Required Standards	**Corresponding GoAnywhere Feature**
Requirement: 5.1(e), 5.2 Personal data shall be processed in a manner that ensures appropriate security of the personal data. The controller shall be responsible for, and be able to demonstrate compliance with, the security.	GoAnywhere has several popular encryption technologies, including AES 256-bit encrypted folders that protect files at rest, ZIP with AES for compressing and encrypting files, OpenPGP compliant encryption that addresses the privacy and integrity of data, and SSH/SSL security for encrypting file transfers. With GoAnywhere, you remain in control of the security of your data at all times. Use detailed reports of file transfer activity, user statistics, and completed jobs to prove compliance with article 5.
Requirement: 7, 8 Individuals must give consent to have their personal data collected and used. Consent must be separable from other written agreements.	Personalize and send your consent forms through GoAnywhere's Secure Forms module. Designate a form as public and send users access with a link, then collect consent and receive files (document scans, form signatures, and so on) as encrypted attachments. All submission history, including date stamps and user responses, is logged for auditing and reports.
Requirement: Article 15, 20 EU citizens may request a copy of data and request to transfer personal data from company to company upon request.	Use GoAnywhere's Secure Forms module to create a data request form. When a user requests a copy of their data, GoAnywhere can encrypt and send the requested information through GoAnywhere's password-protected Secure Mail. This entire process can be completely automated with project workflows.
Requirement: Article 25 Organizations must be able to provide a reasonable level of data protection and privacy.	GoAnywhere provides data protection and privacy through user roles, allowing the admin to limit who can view or process information. It also provides encryption for data in transit and at rest.

Requirement: Article 30 Records of processing activities must be maintained, including the type of data processed and the purposes for which it's used.	GoAnywhere allows you to store and track detailed audit information. It generates comprehensive audit logs of all file transfer and administrator activity, which you can schedule on a regular basis, then search and view through browser-based administration or a PDF report.
Requirement: 32 Controller and processor shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk.	Many GoAnywhere features ensure a stringent level of security for personal data, both in transit and at rest. Use GoAnywhere's encryption technologies, encryption key management, and admin user roles to implement a solid security strategy for your business.
Requirement: 39.1(b), 39.2 A Data Protection Officer shall be able to monitor compliance with the GDPR regulation (assigning responsibilities, related audits).	GoAnywhere's Admin Roles allow you to assign GoAnywhere functions to authorized users. Admin User Roles can be assigned as Auditors or Security Officers, giving you the ability to assign a Data Protection Officer access to whatever they need for monitoring purposes. GoAnywhere MFT is also managed from a single, central location, giving you control over everything without needing multiple logins, products, or unrelated add-ons.

FORTRA

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.