DXRX Security Policy

Last update: 20 July 2023 (Version 2)

Welcome to **DXRX – The Diagnostic Network®** (“**DXRX Network**” or “**DXRX**”).

Unless otherwise stated, any defined terms in here shall have the meaning set out in the **DXRX User Terms.**

Overview

At Diaceutics we take the protection of Your Content extremely seriously. This policy describes the organizational and technical measures Diaceutics implements platform-wide designed to prevent unauthorized access, use, alteration, or disclosure of information. The DXRX Services operate on Amazon Web Services (“**AWS**”). This policy describes activities of DXRX within its instance on AWS unless otherwise specified.

Security Team

Our team consists of people who have played leading roles in the design, build, and operation of highly secure internet-facing systems at companies ranging from start-ups to large public and private companies.

Best Practices

Incident Response Plan

- We have implemented a formal procedure for security events.
- When security events are detected, the relevant Diaceutics’ teams are notified, and assembled to rapidly address the security event.
- After a security event is resolved, we write up a post-mortem analysis.
- The analysis is reviewed by the team, distributed across the company, and includes action items that will make the detection and prevention of a similar event easier in the future.
- Diaceutics will promptly notify you in writing upon verification of a security breach of any DXRX Services that affect Your Content. Notification will describe the breach and the status of Diaceutics' investigation.
- Diaceutics’ data protection, quality and compliance team will also be involved, making their own assessments in line with obligations under applicable Data Protection Law.
- A dedicated communication channel (privacy@diaceutics.com) has been created to handle any queries or breaches related to data protection.

Infrastructure

- All of the DXRX Services are hosted in AWS facilities in the US (Virginia) and in Europe (Dublin) and protected by AWS security, as described at http://aws.amazon.com/security/sharing-the-security-responsibility. DXRX Services have been built with disaster recovery in mind.
- All of our infrastructures are spread across multiple AWS data centers (availability zones) and will continue to work should any one of those data centers fail unexpectedly. Amazon does not disclose the location of its data centers. As such, Diaceutics builds on the physical security and environmental controls provided by AWS. See http://aws.amazon.com/security for details of AWS security infrastructure.
- All of our servers are within our own virtual private cloud (VPC) hosted on AWS with network access control lists (ACLs) that prevent unauthorized requests from getting to our internal network.
- DXRX Services use a backup solution for datastores that contain data.
- We have a continuous integration, continuous delivery, and continuous deployment process in place so that we can safely and reliably roll out changes to both our application and infrastructure in an automated process.

Data

- All Your Content is stored in the US (Virginia) and Europe (Dublin).

- Your Content is stored in multi-tenant datastores; we do not have individual datastores for each DXRX User. However, strict privacy controls exist in our application code that are designed to ensure data privacy and to prevent any unauthorized access between DXRX Users.
- Each DXRX Service system used to process Your Content is adequately configured and pathed using industry-recognized system-hardening standards.
- Diaceutics engages certain **sub-data processors** to process Your Content which is protected by appropriate contracts.

Transfer of Your Content

- All Your Content sent to or from the DXRX Services is encrypted in transit using 256-bit encryption.
- Our API and application endpoints are TLS/SSL only and score an “A+" rating on SSL Labs' tests. This means we only use strong cipher suites and have features such as HSTS and Perfect Forward Secrecy fully enabled.
- We also encrypt data at rest using an industry-standard AES-256 encryption algorithm.

Authentication

- DXRX Services are served 100% over https and run a zero-trust corporate network.
- There are no corporate resources or additional privileges from being on DXRX Services’ network.
- We have two-factor authentication (2FA) and strong password policies to ensure access to the DXRX Network is protected.

Permissions and Administrator Controls

- DXRX Services enable permission levels to be set for any personnel with access to the DXRX Services.

Application Monitoring

- On an application level, we can produce audit logs for all activity.
- All access to DXRX Service applications can be logged and audited.
- VPNs are used for accessing certain sensitive resources.

Security Audits and Certifications

- We use technologies to provide an audit trail over our infrastructure and the DXRX Services application. Auditing allows us to do ad-hoc security analysis, track changes made to our setup, and audit access to every layer of our stack.
- Information about AWS security certifications and obtaining copies of security reports from AWS is available at http://aws.amazon.com/compliance/pci-data-privacy-protection-hipaa-soc-fedramp-faqs/
- To assist with our audits and testing we may choose to bring in external vendors.