tobii dynavox

The Tobii Dynavox E-Funding website Security White Paper

Introduction

For those living in the United States, the Tobii Dynavox E-Funding website allows customers to, in collaboration with its SLP, solutions consultant and other approved parties, to complete and submit a funding packet for a speech generating device (SGD) all online. This helps expedite this step in the funding process and gives access to a place where all documents related to a funding case are stored in one place.

Secure Facility

The eFunding website, backend, and database servers are hosted by Microsoft Azure cloud services that comply with key industry standards, such as ISO/IEC 27001:2013 and NIST SP 800-53, for security and reliability. Physical access to servers is monitored and restricted.

Secure Platform

The Tobii Dynavox E-Funding website utilizes Azure PaaS services, ensuring it runs on the latest Windows environments with up-to-date security patches. These services are managed and hosted by Microsoft Azure, providing robust protection through multi-layer firewalls.

Web Application Firewall (WAF)

To further enhance the security posture of the efunding portal, a Web Application Firewall (WAF) is enabled as part of the Azure App Service deployment. The WAF will provide real-time protection against common web application vulnerabilities, including but not limited to SQL injection, cross-site scripting (XSS), and protocol violations. WAF policies will be configured to align with industry best practices and organizational compliance requirements (HIPAA, GDPR). All WAF events and alerts are monitored and integrated into the organization’s security incident response process. The WAF configuration is reviewed regularly to ensure continued effectiveness and to address emerging threats.

Protecting Customer Privacy

Tobii Dynavox prohibits unauthorized disclosure of user or enterprise customer information to any third party. Our privacy policy identifies the information gathered, how it is used, with whom it is shared, and the customer’s ability to control the dissemination of information.

Protecting user data

All user data stored by The Tobii Dynavox E-Funding website is protected at rest using 256-bit AES (Advanced Encryption Standard) provided by the Azure cloud service.

Access to customer information

Tobii Dynavox staff members are the only individuals with access to Tobii Dynavox servers - limited access is granted on a need-to-know basis for the express purpose of customer support.

Protecting confidential data

The Tobii Dynavox E-Funding website uses a highly compressed, encrypted stream to ensure data confidentiality without sacrificing performance. All traffic between the user's browser and the server is protected with industry standard HTTPS using TLS.

User email addresses

Each user must provide a valid email address to use the system. The email address must be verified by the owner. An email address cannot be used for more than one account.

Password protection and recovery

Users access their account data using their unique username and password. The Tobii Dynavox E-Funding website enforces a minimum password length of 8 characters and displays a password strength indicator when creating or changing a password. Common weak passwords such as "password", "12345678", "abcdefgh" etc. are not allowed. The Tobii Dynavox E-Funding website login screen has a "Forgot Password" link that prompts the user for their email address. If the email address matches the one, we have in the system, an email is sent with a link to allow the user to reset their password.

Conclusion

The Tobii Dynavox E-Funding website protects customer data through industry standard encryption, physically and digitally secure servers, and operational best practices.