LabStyle Innovations HIPAA Compliance Declaration

What is Dario™?

The Dario™ All-in-one smart meter glucose monitoring solution includes a simple-to-use glucose meter, disposable test strip cartridge and lancing device – and comfortably fits in your pocket. Connecting to your mobile device, the smart meter makes it easy to manage your health, automatically log results, and always stay connected with your caregiver and health care provider.

Dario™ is a state-of-the-art diabetes management platform that connects the user, caregiver and healthcare professional through Dario's™ cloud-based software. Dario™ provides you with an easy seamless way to record, save, track, analyze, manage and share all your diabetes related information in one lifestyle management platform. Through the Dario™ web portal you can access all your activity and medication data. Your data is always in sync and always accessible on-line in a user-friendly interface via a secure Web session. The Dario™ Web Portal is an easy way to share your profile with caregivers and family members at your discretion.

Background

When handling sensitive medical and personal information through mobile medical apps and cloud based data collection – and their ever-increasing integration with social media outlets such as Facebook – implementing proper security measures and compliance with HIPAA (Health Insurance Portability and Accountability Act) regulations is of the utmost priority for Dario's™ mobile healthcare technology.

Security Standards for the Protection of EPHI (Electronic Protected Health Information) are provided by the Centers for Medicare and Medicaid Services (CMS). The guidance that CMS provides for security measures is defined in 45 CFR Parts 160 and 164 Subparts A and C – also known as the Security Rule, which executes the requirements for data protection in HIPAA. The Security Rule details specific requirements for security safeguards. Items marked *(R)* are required and items marked *(A)* need to be addressed according to the results of the risk analysis.

Risk analysis, Audit controls, and Transmission security

The first required safeguard in the Security Rule is a risk analysis - *"As part of the risk management process, the company performs an annual risk analysis for its products analyzing software and data security"*. The Security Rule details specific requirements for security safeguards. The Audit Controls protections require that to *"Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information."* Transmission security precautions require a covered entity to: *"Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network."*

To this extent, Dario™ performs annual third-party security audits of their servers to make sure that all of the personal and medical information is being kept safe. In addition, Dario™ stores personal data and medical data separately. Therefore, there is no way to match the medical information or condition with a particular person. All of the data on your mobile device and in the cloud are encrypted by the Dario™ user's log-in credentials.

Person or Entity authentication (R)
This safeguard requires a covered entity and its suppliers to *"Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed."*

Only the Dario™ user can share their information with intended parties. Caregivers or healthcare professionals can only access the Dario™ users' information when the user chooses someone from their contacts or manually enters their email address to send them an email.

Access control
The Security Rule defines access as *"the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource"*.

Dario™ has implemented access control such as a unique user identification for end users in the Dario™ mobile app and website for system administrators and software developers. Dario™ users are able to recover their password and access their data through the mobile

app and website. After a specified amount of inactivity, the mobile app automatically logs off. EPHI is stored separately from personal and medical information and is encrypted on the server.

Mobile device policy

In the event a user has a lost or stolen mobile device, a Dario™ user can log in using their personal credentials through the Dario™ website and change their password. Once the password is changed on the Dario™ website, someone trying to access the data from the mobile device will not be able to access the information once the password has been changed. Users of Dario™ are encouraged to use their mobile device's own security settings, such as locking the screen after a period of inactivity with a password to provide an additional layer of protection if they feel it is necessary.

Summary

Dario™ has implemented the appropriate Security Rule safeguards as part of a corporate commitment to protecting personal data through a strong security and compliance management program.