P2721

Submitter Email: dklonoff@diabetestechnology.org
Type of Project: Modify Existing Approved PAR
PAR Request Date: 12-Mar-2019
PAR Approval Date: 21-May-2019
PAR Expiration Date: 31-Dec-2021
Status: Modification to a Previously Approved PAR
Root PAR: P2721 **Approved on:** 28-Sep-2017
Project Record: P2721

1.1 Project Number: P2721
1.2 Type of Document: Standard
1.3 Life Cycle: Full Use

2.1 Title: Standard for Wireless Diabetes Device Security Assurance

Changes in title: Standard for Wireless ~~Health~~Diabetes Device Security Assurance

3.1 Working Group: Healthcare Device Security Assurance Working Group (EMB/Stds Com/HDSecWG)
Contact Information for Working Group Chair
Name: David Klonoff
Email Address: dklonoff@diabetestechnology.org
Phone: David Klonoff
Contact Information for Working Group Vice-Chair
None

3.2 Sponsoring Society and Committee: IEEE Engineering in Medicine and Biology Society/Standards Committee (EMB/Stds Com)
Contact Information for Sponsor Chair
Name: Carole Carey
Email Address: c.carey@ieee.org
Phone: 301-776-9882
Contact Information for Standards Representative
None

4.1 Type of Ballot: Individual
4.2 Expected Date of submission of draft to the IEEE-SA for Initial Sponsor Ballot: 02/2020
4.3 Projected Completion Date for Submittal to RevCom
Note: Usual minimum time between initial sponsor ballot and submission to Revcom is 6 months.: 08/2020

5.1 Approximate number of people expected to be actively involved in the development of this project: 25

5.2 Scope: This standard specifies the security assurance requirements for wireless diabetes devices. These requirements are codified by the use of protection Profiles and Security Targets in this standard for the following:
* To establish the general requirements for connected diabetes devices that meet the balanced needs for security and clinical application.
* To identify possible and potential threats related to the various components and interfaces of the connected diabetes devices, such as network, storage, software, connected peer devices, and cryptography.
* To define a set of generalized requirements that apply to families of similar devices
* To define a set of specific mandatory requirements, derived from the generalized requirements, corresponding to specific connected diabetes device products and components.
* To outline additional optional functional requirements for manufacturers to consider adding to their products for future development.

Changes in scope: This standard specifies the security assurance requirements for wireless ~~healthcare~~diabetes devices. These requirements are codified by the use of protection Profiles and Security Targets in this standard for the following: * To establish the general requirements for connected diabetes devices that meet the balanced needs for security and clinical application. * To identify possible and potential threats related to the various components and interfaces of the connected diabetes devices, such as network, storage, software, connected peer devices, and cryptography. * To define a set of generalized requirements that apply to families of similar devices * To define a set of specific mandatory requirements, derived from the generalized requirements, corresponding to specific connected ~~healthcare~~diabetes device products and components. * To outline additional optional functional requirements for manufacturers to consider adding to their products for future development. In addition to the creation and approval of security requirements documents, this standard also defines the assurance program for evaluating and certifying products against those requirements.

In addition to the creation and approval of security requirements documents, this standard also defines the assurance program for evaluating and certifying products against those requirements.

5.3 Is the completion of this standard dependent upon the completion of another standard: No
5.4 Purpose: This document will not include a purpose clause.
5.5 Need for the Project: Medical devices used for monitoring and managing diabetes provide life-saving benefits to patients and effective implementation options to healthcare providers. These devices include blood and continuous glucose monitors, insulin pumps, pens and other insulin delivery devices, and closed loop artificial pancreas systems and others. With ever-increasing connectivity and data exchange between these diabetes devices, other devices (such as smart phones), and the Internet, there is an increased risk to the safety and privacy of the patient and to the integrity of the healthcare provider.

5.6 Stakeholders for the Standard: Device Manufacturers, Clinicians, Regulators, Certification Bodies, Independent Cybersecurity/Privacy Experts, Healthcare Facilitators, test labs, software developers

---

Intellectual Property
6.1.a. Is the Sponsor aware of any copyright permissions needed for this project?: Yes
If yes please explain: The basis of this standards will be the Diabetes Technology Society standard DTSec.

6.1.b. Is the Sponsor aware of possible registration activity related to this project?: No

---

7.1 Are there other standards or projects with a similar scope?: Yes
If Yes please explain: UL 2900
The UL 2900 series of standards consists of the following parts, under the general title 'Standard for Software Cybersecurity for Network-Connectable Devices':

Part 1: General Requirements for Network-Connectable Devices
Part 2-1: Particular Requirements for Healthcare Systems
Part 2-2: Particular Requirements for Industrial Control Systems
Part 3: General Requirements for the Organization and Product Development Security Lifecycle Processes for Network-Connectable Devices

and answer the following
Sponsor Organization: UL
Project/Standard Number: UL2900
Project/Standard Date:
Project/Standard Title: Cybersecurity for Network Connected Diabetes Devices
7.2 Joint Development
Is it the intent to develop this document jointly with another organization?: Yes
Organization: Underwriter Laboratories
Technical Committee Name: n/a
Technical Committee Number:
Contact Name: Sonya Bird
Phone: 919.549.1685
Email: sonya.m.bird@ul.com

8.1 Additional Explanatory Notes: IEEE and UL have signed an MOU for joint developm

2.1 and 5.2: The connected devices used in diabetes might have different properties and different vulnerabilities than connected devices used for other diseases. We intend to build this standard for diabetes first. This standard might be useful as a template for connected devices for other diseases in the future. We feel that this project is more likely to be successful if we focus on diabetes devices rather than devices for all types of health conditions.