DriveSafe DriveAware

Architecture and Security Reference

Version 1.0

Date created: April 2015

1. Introduction

DSDA assesses a driver's awareness of the driving environment and their own abilities related to driving. It is a cognitive screening tool that can be used for drivers with a wide range of medical conditions that impact cognitive capacity for driving. DSDA can be used as a decision support tool for doctors and other health professionals when determining whether referral for an on-road assessment is necessary. Administration takes place via an app on an iPad, where the patient records their responses.

Maintaining a secure infrastructure and environment that safeguards data and personally identifiable information is our highest priority for our customers. This document will focus on the architecture and security that is employed by DriveSafe DriveAware (DSDA) to safeguard such data.

A. Dedicated Firewall

A dedicated firewall provides the first line of defence and controls traffic between trusted and untrusted networks. It filters and blocks non-essential traffic based on ports and protocols, allowing only wanted and appropriate traffic into the private network.

B. Load Balancer

Load balancers provide redundancy and manage platform load, but they also manage traffic and obfuscate the endpoint to help protect against insertion and evasion network attacks. They enable HTTPs session persistence across servers to ensure data is transferred securely across DSDA.

C. Log Management

Log management helps in detecting unauthorised access attempts. The systems perform specific event logging at the application layer to help identify potential attacks, allowing appropriate monitoring and response..

D. Vulnerability and Penetration Testing

Vulnerability and Penetration Testing is regularly conducted and allows for the identification of exploitable weaknesses. It can be performed at different intervals to ensure that configuration changes, patches or functionality enhancements did not introduce exploitable weaknesses. This testing is a proactive, preventative control that enables the finding and addressing of application and infrastructure weaknesses.

E. Data Encryption

The Personally Identifiable Information (PII) collected includes only the information you provide about your patient/client when completing the Patient Record. This may include name, date of birth, address, medical diagnoses and medical record numbers.

Pearson protects personal data with:

- Administrative safeguards,
- Physical safeguards, and
- Technical safeguards.

This is achieved as follows:

1. In Transit

All data that is transferred between the DSDA app is transmitted using 128-bit SSL connections. The web browser validates the HTTPs certificate and generates an exception if the certificate is not valid.

2. At Rest

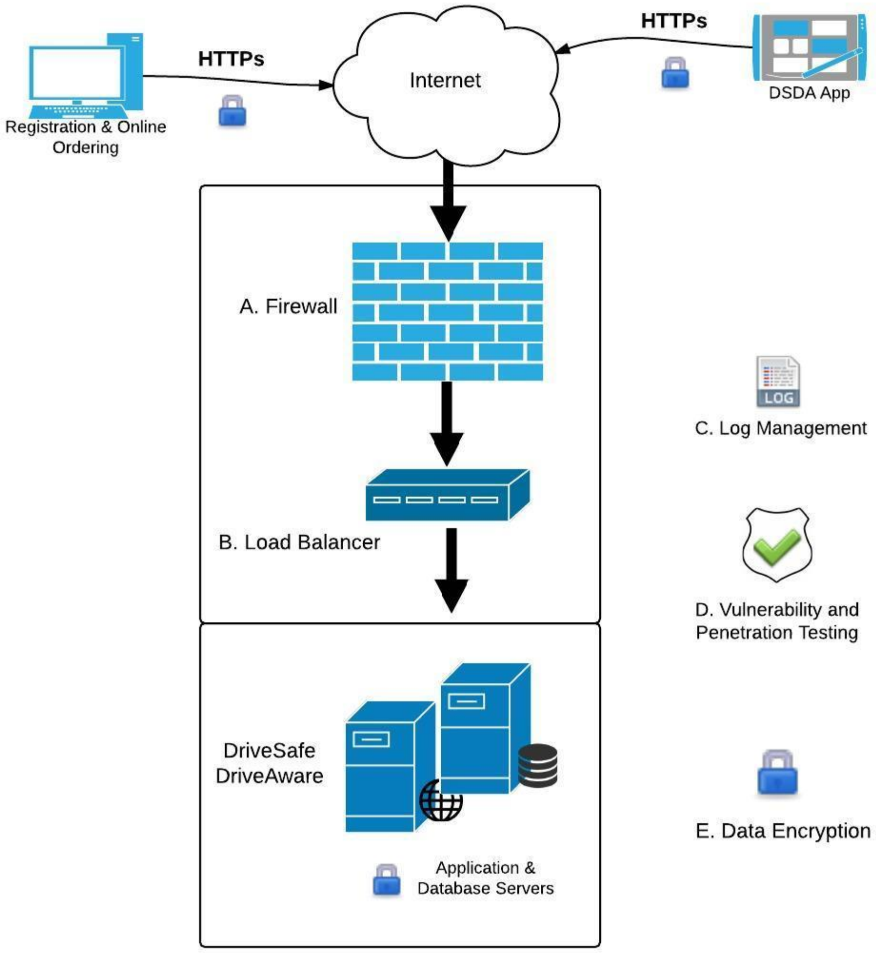
DSDA client data is encrypted in a database that is hosted in a dedicated, secure environment in Melbourne, Australia. This environment is restricted and physical and virtual access is restricted to authorised personnel only.

3. On Device

DSDA client data is encrypted on all devices that have the iOS ‘Passcode’ setting activated. The DSDA app will alert the user to activate this setting when first installed on a device.

Please read Pearson’s Data Security and Privacy Policy here.

Diagram 1 – Architecture Overview


HTTPs
Internet
HTTPs
Registration & Online Ordering
DSDA App
A. Firewall
B. Load Balancer
C. Log Management
LOG
D. Vulnerability and Penetration Testing
DriveSafe DriveAware
Application & Database Servers
E. Data Encryption