

**Senate Community Affairs Committee**

**ANSWERS TO ESTIMATES QUESTIONS ON NOTICE**

**HEALTH PORTFOLIO**

**Budget Estimates 2014 - 2015, 2/3 June 2014**

**Ref No:** SQ14-000501

**OUTCOME:** 7 - Health Infrastructure, Regulation, Safety and Quality

**Topic:** eHealth Implementation Issues

**Type of Question:** Written Question on Notice

**Senator:** Xenophon, Nick

**Question:**

Both the National E-Health Transition Authority (NEHTA) and the Department of Health have indicated that they are aware of the potential security vulnerabilities of eHealth systems.

Can you indicate whether you have trialled any of the listed controls and protection mechanisms on real-life test cases?

**Answer:**

To secure and protect personally controlled electronic health records, the Personally Controlled eHealth Record (PCEHR) system operator has implemented bank-strength security features including strong encryption and firewalls, secure logins and audit trails. These protections are consistent with the Australian Government's Protective Security Policy Framework & standards issued by the Australian Signals Directorate - Department of Defence.

The system operator manages potential security vulnerabilities in accordance with the Australian Government's Information Security Manual's standards on vulnerability management. The system operator engages an independent expert vulnerability assessor to regularly assess the effectiveness of the controls and mechanisms protecting the national infrastructure. The vulnerability assessor develops test cases from current best practise, which includes test cases based on known "real-life" vulnerabilities and attacks. Any identified vulnerabilities are then assessed for their impact on the eHealth program, and appropriately mitigated or treated as soon as possible.