

MEMORANDUM

To: Rep. Martha Heath, Chair, House Committee on Appropriations

From: Mark Larson, Commissioner

Cc: Doug Racine, Secretary, Agency of Human Services

Date: April 19, 2013

Re: Health Benefit Exchange - Cloud Computing Privacy and Security

During DVHA's testimony on the Health Benefit Exchange financing for 2015 and beyond to the House Committee on Appropriations, committee members requested information on the privacy and security measures the Health Benefit Exchange was undertaking with respect to its cloud computing contract.

The following is a summary of the privacy and security measures outlined in the state's contract with CGI for cloud computing services:

- National Institute of Standards & Technology 800 Series Requirements
- The Health Insurance Portability and Accountability Act (HIPAA)
- Health Information Technology for Economic and Clinical Health Act (HITECH)
- Payment Card Industry (PCI) Data Security Standards
- IRS 1075 Requirements
- State of Vermont Security Policies and Standards
- Federal Information Processing Standard (FIPS)
- Federal Information Security Management Act (FISMA)

CGI will also be required to conduct a Statement on Standards for Attestation Engagement (SSAE) No. 16; Service Organization Control (SOC) 2 audit annually and provide the results of that audit to the State of Vermont. In addition to these contract measures the Health Benefit Exchange is currently drafting a Privacy Impact Assessment (PIA) to be submitted to CMS by May 15th. Conducting a PIA facilitates the identification of systems that contain personally identifiable information (PII) and satisfies system compliance with all relevant privacy laws, regulations, and guidance.

If you should have any questions please do not hesitate to contact me.