

## Office of Security Services – Design Review Guidance

*The HCA Office of Security Services must review all system implementation and upgrade projects for security and compliance issues.  
HCA Policy 6-16, 1.d.ii*

### Overview

No area within IT is changing more rapidly than cybersecurity. The quantity and severity of security threats grows constantly. To combat this growing threat, the State of Washington performs Security Design Reviews, which are conducted by Washington Technology Solutions (WaTech). The Office of Security Services (OSS), a section within the Health Care Authority's Enterprise Technology Services (ETS) division, in partnership with The Office of CyberSecurity (OCS) at WaTech, is responsible for reviewing all system implementations and upgrades for compliance with federal and state regulations. These reviews will determine whether organizations receiving HCA data are compliant with established standards for transmitting, storing and using electronic private health information (ePHI).

### Process

Contact the ETS Office of Security Services when a project:

- Implements new technology
- Upgrades existing technology
- Shares data with new entities or by new mechanisms

To contact OSS, submit a ticket to the Help Desk. OSS will evaluate the project and determine security and compliance requirements. For example, an internal design review may be adequate for some projects, while a complete OCS/OCIO Security Design Review may be required for others.

If a complete OCS design review is necessary, OSS will provide guidance and coordinate the OCS Security Design Review process.

### Considerations

For OSS to efficiently move projects through the process, documentation will be requested from any new entities involved in the project. Examples of documentation could include system diagrams, security policies and procedures, and SSAE 16 SOC 2 Type II reports.

Depending on the project, legal documentation such as a Business Associate Agreement, Contract, or Data Sharing Agreement may also be required. OSS does not author nor maintain these documents, but will assist in the development of any security-related language. Contracts staff are aware of this requirement and stand ready to ensure that contracts are executed properly. For example, one important point for such documentation is that it must bind external entities to comply with [OCIO Standard 141.10, Securing Information Technology Assets Standards](#).

The OCS Design Review calendar is full due to the large volume of Design Reviews being conducted by state agencies. The current wait time for an OCS review is 3-4 months, and it typically takes an outside entity 2-8 weeks to provide the required documentation. Contact OSS about your project as early as possible in its development to minimize delay.

Cybersecurity is everyone's responsibility. OSS is continually improving the process detailed here and would appreciate feedback to support the vision of a *Healthier Washington*.

### **Questions?**

Should you have questions, please contact Bill Brush, HCA's Chief Information Security Officer at [bill.brush@hca.wa.gov](mailto:bill.brush@hca.wa.gov) or at 725-5148.