SDSC Sherlock Cloud: Secure, Compliant & Managed Cloud Services

Cloud computing allows users to scalably store and manage data in a secure online environment. This fosters the deployment and management of new projects without a large investment of time, cost, or infrastructure. Moreover, cloud resources can be tailored to an individual project’s needs while leveraging economies of scale and shared expertise. Sherlock Cloud (http://sherlock.sdsc.edu), an offering of the SDSC Health Cyberinfrastructure Division, incorporates these philosophies and provides secure data storage, application hosting and computing capabilities to academic and government partners.

Sherlock Cloud was developed in accordance with hundreds of National Institute of Standards and Technology (NIST) controls that govern system access, information control and safeguarding, and management processes. Additionally, Sherlock Cloud complies with the Health Information Portability and Accountability Act (HIPAA) and Federal Information System Management Act (FISMA); it currently supports the National Institutes of Health (NIH), Centers for Medicare & Medicaid Services (CMS) and a number of University of California (UC) institutions (UCOP, UCSF & CalIT2).

While Sherlock Cloud currently supports NIH, CMS and the UC, it has the foundation to also partner with various organizations, departments and researchers seeking to capitalize on Sherlock Cloud’s expertise in supporting HIPAA environments. In regard to Sherlock Cloud’s HIPAA expertise, it has developed a managed IT/cloud services framework to ensure secure and compliant hosting services for sensitive Protected Health Information (PHI) data. The benefits of Sherlock Cloud’s managed IT/cloud services include:

- Highly technical and experienced staff;
- Varying levels of domain knowledge;
- Good economies of scale;
- Great industry knowledge;
- Formal IT and security processes; and
- Common policies and templates.

Sherlock Cloud not only provides current and potential partners the benefits of its managed IT/cloud services, but it meticulously follows stringent guidelines and policies required to maintain HIPAA-compliant status, thereby safeguarding the sensitive PHI data. Sherlock Cloud’s HIPAA compliance involves managing the entire software and hardware platform and the necessary management processes. Accordingly, Sherlock Cloud’s management, security, and systems teams continuously monitor, regularly test, and actively maintain the requirements including, but not limited to:

- Generating and maintaining policy and lifecycle documents (System Security, Incident Response, Contingency, etc.);
- System vulnerability scanning, flaw remediation, continuous system monitoring and log analysis;
- Conducting yearly security assessments and security testing for all staff with access to HIPAA data;
- Testing regularly for purposes of backup/archiving;
- Performing workforce clearances and background checks;
Monitoring physical security controls, access controls and authentication; and

Ensuring data transmission security and data at rest security.

**OUR APPROACH**

Sherlock’s team of information technology specialists guide partners through the process of determining and understanding the steps necessary to meet and maintain their HIPAA-compliant hosting needs. Specifically, the team has developed a framework to gather the requisite information to ensure proper planning, deployment, and maintenance of a project.

**Step 1: Determining Project Background and Scope**
Before a project can be initiated, the Sherlock Cloud team must understand the project’s background and scope. Moreover, the project’s regulatory requirements (i.e., HIPAA) and security requirements and parameters must be identified. Armed with this information, it can then be determined how the Sherlock Cloud team can assist the partner with its project.

**Step 2: Understanding Project Compliant Hosting Requirements**
The Sherlock Cloud team must become familiar with the project’s compliant hosting requirements, which requires the partner to detail specific technical requirements of the project (e.g., applications, compute and storage, service-level agreements, etc.).

**Step 3: Proposing and Building a Platform**
Next, the Sherlock team will jointly work with its partner to propose and architect the platform. This step entails outlining the system architecture for project deployment within Sherlock Cloud, defining and testing a Proof-of-Concept implementation, discussing costing options, developing a Memorandum of Understanding outlining deliverables, roles and responsibilities and service level agreements, and initiating platform deployment upon contract award.

**Step 4: Providing Ongoing Operations and Maintenance Support**
Finally, the Sherlock team will work with its partner to maintain compliance requirements and provide ongoing operations and maintenance. Examples of ongoing managed operations and maintenance include: infrastructure support, system administration and maintenance, change management, security/CISO support, and project management and coordination.

Sherlock Cloud was built to support researchers and their projects, and understands the requirements of research computing and how the needs of researchers and investigators may differ from those of the typical end users of commercial cloud platforms. Sherlock Cloud offers the ability to partner on a project basis, improving economies of scale based on shared infrastructure, processes, and documentation, and providing expertise in supporting FISMA and HIPAA environments. Sherlock Cloud provides researchers a competitive advantage in their proposals, in the execution of their awards, and in the ongoing enhancement of their capabilities. The Sherlock Cloud team strongly believes that it can provide a valuable service and serve a critical need for Federal, State, and Private partners.