Cloud Security with the NAVIFY Tumor Board solution


Trust that your oncology patients’ healthcare information stays protected.
In the era of precision medicine, you can keep patient data secure and accessible to the right specialists.

Security breaches are on the rise

In 2017, huge data breaches in systems such as Indiana Medicaid (1.1 million enrolled patients) and Molina Healthcare (4.8 million patient records compromised) continue to affect the integrity of healthcare systems and expose major vulnerabilities in their security protocols.¹ ²

HIPAA privacy and security breaches are on the rise, costing the U.S. healthcare industry an estimated $6.2 billion per year.

One recent survey found that nearly one-third of patients would change caregivers if their protected healthcare information was breached.¹
The NAVIFY Tumor Board solution is built to keep healthcare data safe

Healthcare organizations face many unique challenges when it comes to their technology, which is why adopting purpose-built cloud-based solutions is becoming an industry-wide best practice. Cloud deployment allows access to expansive resources and expertise, is flexible enough to scale or integrate with other hospitals’ systems, and most importantly, runs regular, fully-tested system safety checks for protection against the latest cybersecurity threats.

Roche built the NAVIFY Tumor Board solution from the ground up to be deployed and hosted in the cloud, partnering with industry leader ClearDATA to ensure protected health information (PHI) remains secure. The NAVIFY Tumor Board solution is built around safeguarding all the different kinds of sensitive data being entered into it, including patient data from EMRs, imaging data from PACS, laboratory results, etc.
Delivering best practices—securing data in the cloud

When moving computer systems and data to the cloud, security becomes shared between the software and the cloud service provider. This shared model can reduce operational burden and assure data is only accessible by authorized users.4

As the diagram below shows, ClearDATA provides a managed service to host the NAVIFY Tumor Board solution on the Amazon Web Services (AWS) infrastructure. AWS takes responsibility for securing the underlying infrastructure that supports the cloud, and the actual physical hardware needed to do so. ClearDATA then controls what gets deployed into the infrastructure, audits who accesses the infrastructure, and monitors what is happening in the infrastructure. The multi-tier authentication established by its cloud service providers help the NAVIFY Tumor Board solution add layers of protection on top of the traditional username and password.
Certified and dependable cloud partners

Amazon Web Services (AWS) serves several of the world’s largest healthcare companies with their cloud infrastructure. Roche chose to partner with AWS to leverage their experience with meeting security and privacy requirements that help safely manage PHI in the cloud. In addition, Roche has also partnered with ClearDATA, who builds their capabilities on top of AWS. More than 350,000 healthcare professionals trust ClearDATA to protect their patient data and power the back end of their critical applications.5

ClearDATA is certified by the Health Information Trust Alliance (HITRUST)6 to be flexible and efficient enough to rationalize the industry’s mandatory regulations and standards within its security framework. And its ISO 27001 certification6 can help assure that any changing security needs in the future are managed on an ongoing basis in a holistic, comprehensive manner.

<table>
<thead>
<tr>
<th>Certification/Compliance</th>
<th>Infrastructure (ClearDATA)</th>
<th>The NAVIFY Tumor Board solution (Roche)</th>
</tr>
</thead>
<tbody>
<tr>
<td>HIPAA</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>HITRUST</td>
<td>✓</td>
<td>2018*</td>
</tr>
<tr>
<td>ISO 27001</td>
<td>✓</td>
<td>2018*</td>
</tr>
</tbody>
</table>

*Estimated.
Why the cloud over on-premise systems?

While some IT healthcare professionals worry that the cloud is not as secure as on-premise IT resources and servers, investigations into the highest-profile and most costly data breaches have found that the entry points existed within on-premise company firewalls, rather than at cloud infrastructure points.⁷

Cloud platforms not only undergo rigorous penetration testing and allow for a more rapid response to security issues, but also offer various operational advantages that help healthcare IT systems run more smoothly. Systems built using cloud services can support rapid development and innovation to help prepare IT systems for growth and the future needs of care teams.⁸

For example, the ability to share healthcare information between care specialists easily and securely is crucial for optimal care, and cloud services are good enablers of streamlined communication. Unlike on-premise systems, the cloud offers users remote access to applications and data at anytime from anywhere, introducing global collaboration possibilities for multidisciplinary teams.

HEALTHCARE DATA IN THE CLOUD

Over 75% of surveyed healthcare organizations either have their PHI data in the cloud, or anticipate migrating to the cloud in the near future.⁹
Moving to the cloud provides more expansive resources for collaboration to help improve outcomes, and protects against the latest, ever-evolving threats of a data breach.
To learn more, visit us at **NAVIFY.com/tumorboard.**

References


Diagnostics Information Solutions (DIS)
Roche Molecular Systems, Inc.
1301 Shoreway Road, Suite 300
Belmont, CA  94002
NAVIFY.com/tumorboard
© 2017 Roche Molecular Systems, Inc.