Industry Snapshot: Cloud Security in Healthcare
Solid Industry Growth

WW Public Cloud Service Revenue ($B)

- **IaaS**: $176B (16.5% CAGR) to $278B in 2021
- **SaaS**: ~$5B to ~$10B
- **PaaS**: ~$176B to ~$278B
- **BPaaS**: ~$176B to ~$278B
- **Cloud Mgmt/Security Services**: ~$176B to ~$278B

IaaS fastest growing with 26.7% CAGR; doubling revenue by 2021

Global Cloud Computing Healthcare Revenue ($B)

- 22% CAGR by 2022
- ~$5B to ~$10B

Sources:
- "Technavio, August, 2018; "Frost & Sullivan, September, 2018"
Online survey conducted by HIMSS Media on behalf of the Center for Connected Medicine among 100 U.S. hospitals and health systems to better understand attitudes and perceptions about cloud security.

Qualified respondents included a mix of IT, Cybersecurity and Informatics professionals.

### Source
HIMSS Media Cloud Security Insights Research, 2018, Sponsored by:
## Key Takeaways

<table>
<thead>
<tr>
<th></th>
<th>Rapid acceleration for cloud adoption continues.</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>With mission-critical workloads making up a growing share of cloud portfolios.</td>
</tr>
<tr>
<td>3</td>
<td>Cybersecurity concerns are limiting cloud usage.</td>
</tr>
<tr>
<td>4</td>
<td>But are security concerns warranted?</td>
</tr>
<tr>
<td>5</td>
<td>Evidence of growing trust in security of public clouds but will workloads follow?</td>
</tr>
</tbody>
</table>
Cloud Adoption Continues to Accelerate

Average % of healthcare IT workloads deployed on-premises versus in the cloud

- 12 Months Ago*: 21% cloud, 79% on-premises
- Today: 39% cloud, 61% on-premises
- In 12 Months: 50% cloud, 50% on-premises

Active Investment in Cloud Applications

- **Investing in new, non mission-critical cloud applications**: 78% frequently/occasionally
- **Investing in new, mission-critical cloud applications**: 68% frequently/occasionally

Source: HIMSS Media Cloud Security Insights Research, 2018, Sponsored by Center for Connected Medicine
Mission-Critical Workloads
Growing Share of Cloud Portfolio

Average HIT Cloud Workload Split Today

Mission-critical workloads, 53%

Back-end, non-critical workloads, 47%

Source: HIMSS Media Cloud Usage in Healthcare: Preparing for the Next Wave, 2019
De-identified EHRs: 88%
Info from general business apps: 81%
Medical images: 80%
Patient registries: 77%
Genomics data: 74%
Physician notes: 74%
Electronic health records: 73%
PII related to patient billing, scheduling, registrations: 73%
Internal confidential info like board meeting minutes: 70%
Personalized staff information: 69%

Source: HIMSS Media Cloud Security Insights Research, 2018, Sponsored by Center for Connected Medicine
Extent to which cybersecurity concerns are limiting use of cloud services
(7=Significantly limiting; 1=Not limiting)

- Significantly limiting (6,7 rating): 26%
- Somewhat limiting (4,5 rating): 56%
- Not limiting (1, 2, 3 rating): 18%

Large hospitals (>500 beds) are nearly 2x as likely to report security concerns significantly limit cloud usage

Source: HIMSS Media Cloud Security Insights Research, 2018, Sponsored by Center for Connected Medicine
Do Security Concerns Match Reality?

Fewer than 10% report known security incidents linked to cloud

- Experienced security incidents linked to cloud past 12 months:
  - Unsure, 28%
  - Yes, 7%
  - No, 65%

Source: HIMSS Media Cloud Security Insights Research, 2018, Sponsored by Center for Connected Medicine
Denial of service attacks
Insider theft/misuse of data
Lack of consistent controls to secure multi-cloud & on-premise
Cloud workloads created outside of IT (shadow IT)
Inability to monitor workloads/apps for vulnerabilities
Lack of staff with cloud security skills
Malware infections
Lack of visibility re: where data is stored
Advanced persistent threats/attacks
Identity/access management
Data theft by malicious actor

Source: HIMSS Media Cloud Security Insights Research, 2018, Sponsored by Center for Connected Medicine
Cloud Security Concerns Vary by Organization Size

<table>
<thead>
<tr>
<th>Issue</th>
<th>Hospitals &gt;500 beds</th>
<th>Hospitals 500 or fewer beds</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identity/access management</td>
<td>54%</td>
<td>41%</td>
</tr>
<tr>
<td>Lack of visibility regarding where data is stored</td>
<td>43%</td>
<td>30%</td>
</tr>
<tr>
<td>Inability to monitor workloads/apps for vulnerabilities</td>
<td>43%</td>
<td>27%</td>
</tr>
<tr>
<td>Cloud workloads created outside of IT (shadow IT)</td>
<td>43%</td>
<td>25%</td>
</tr>
<tr>
<td>Lack of consistent controls for securing multi-cloud &amp; on-premise</td>
<td>43%</td>
<td>25%</td>
</tr>
<tr>
<td>Denial of service attacks</td>
<td>29%</td>
<td>14%</td>
</tr>
</tbody>
</table>

Source: HIMSS Media Cloud Security Insights Research, 2018, Sponsored by Center for Connected Medicine
Are Providers Doing Enough to Protect Data in the Cloud?

- Establishing business associate agreements: 48%
- Adopting cybersecurity practices*: 48%
- Establishing policies to manage data access: 42%
- Establishing rules around provider encryption practices: 40%

Source: HIMSS Media Cloud Usage in Healthcare: Preparing for the Next Wave, 2019

* i.e., multifactor authentication
Trust in Public Cloud

2/3rds trust public cloud solutions to keep data secure

Trust public cloud solutions to keep healthcare systems & data secure

- 20% Still unsure
- 18% No
- 55% Yes, for some applications/workloads
- 7% Yes, without hesitation

Source: HIMSS Media Cloud Security Insights Research, 2018. Sponsored by Center for Connected Medicine
Healthcare Data Comfortable Storing in **Public Cloud**

- De-identified EHRs: 52%
- Info from general business apps: 34%
- Patient registries: 30%
- Medical images: 29%
- Genomics data: 29%
- Proprietary company documentation and IP: 25%
- Internal confidential info like board meeting minutes: 25%
- PII related to patient billing, scheduling, registrations: 24%
- Electronic health records: 20%
- Government identification information like SSN: 19%

Source: HIMSS Media Cloud Security Insights Research, 2018, Sponsored by Center for Connected Medicine
Average percent of workloads deployed in cloud has nearly doubled in last year, and is expected to hit the tipping point in 12 months.

Mission-critical workloads account for more than 50% of cloud deployments today on average, and with 2/3rds investing in new mission-critical cloud applications continued growth is likely.

8 out of 10 report cybersecurity concerns are limiting cloud usage but fewer than 10% report known security incidents linked to cloud.

Data theft, compliance and identity access management are key cloud security concerns but fewer than 50% are taking steps to mitigate these concerns.

Majority trust public cloud solutions to keep data secure, at least for some applications, but only a minority are comfortable storing most healthcare data in the public cloud.
For more information about the Center for Connected Medicine, please visit [www.connectedmed.com](http://www.connectedmed.com).