Digital Trust | Earn it and Sustain it to Fuel Tomorrow's Healthcare

By: David Devine

Consumers upload their credit card to mobile devices, give websites access to their location and provide email addresses to retailers. Consumers trust that these mediums are secure for sharing information, allowing businesses to use this data to build customer relationships and drive growth. Healthcare organizations must earn the right to do the same.

Digital trust, the confidence consumers have in an organization to keep their information secure, takes years to earn, but can evaporate in a matter of moments. A data breach can do just that, tarnishing a brand's reputation as consumers lose trust and chose other institutions for their care. For healthcare institutions, a data breach costs $3.7 million in lost revenue.

Digital Trust Starts With Brand Building

When consumers give a brand their information, they expect that organization to use it judiciously and protect it. In the case of Apple, this means safeguarding identifiable information from hackers while at the same time using it to create a more personalized experience by recommending mobile apps based on download history and leveraging location information to share restaurants in the area.

Consumers' trust in a healthcare organization begins before they show up for an appointment or procedure. While awards and accolades are important to building your image, marketing emails, signage, customer service staff and reputation are also key contributors. For consumers to choose your hospital and trust you with their medical information, you must deliver a consistent message through every customer touchpoint and interaction. Impersonal, mass emails do little to inspire consumers that their information is being used to their benefit, let alone that it's secure.

In this give-and-take relationship, organizations must prove the value they bring in exchange for consumers' information or risk eroding their trust.

If You Have Data, You Must Protect It

Whether data is housed on premise or in a public or private cloud, it is critical that you ensure security measures are in place and identify potential risks before hackers capitalize. This behind-the-scenes work earns you the right to shine a light on patient safety and care outcomes that distinguish your brand, without worrying that they'll be overshadowed by data breaches that negate consumer trust.

As the cloud transitions to replace on-premise data centers, data is more accessible, but these periods of transition bring risk. To enhance security, a multi-faceted approach that identifies areas of risk through app and network penetration testing for both on-premise and cloud-based data storage is critical.

In addition, conducting comprehensive security risk analyses must be a regular occurrence.

A security risk analysis should include the following steps:

1. **Design and assess the current state:** Assess and plan for the analysis by identifying key stakeholders. Collect critical information regarding governance, budget, hardware, network design, help desk processes, security policies and risk management, and application portfolio and support structure.
2. **Implement cybersecurity analytics:** Collect, aggregate and analyze security data in order to develop algorithms that can identify the threat before it impacts your business.
3. **Track metrics and create a roadmap for improvement:** Develop a scorecard that includes areas of priority, resources needed for improvement and timeliness for implementation. This allows you to measure progress toward best practices.

By investing in data security and cyberattack prevention, your organization can focus on using data to better engage with patients and to make innovative concepts a reality.

What Digital Trust Means For the Future of Healthcare

The success of precision health and genomics in the provider space require consumers be comfortable with the security of their unique genomic data. As health systems move towards branding around precision medicine building trust today is vital.

In January 2018, India's biometric database that held personal information on 90 percent of its citizens was hacked. Massive data repositories like this are critical for putting big data into action, but consumers must believe that their data is safe before offering up their information.

At the same time, Apple is launching an update to its Health app that will aggregate a patient's medical information from various healthcare systems into a single health record. For patients to use this feature, they must not only trust their providers to securely store their information, but also trust Apple to do the same. As other technology giants like Google and Microsoft make investments in healthcare technologies, data security enhancements must continue to be a high priority for healthcare organizations.

Gaining and sustaining digital trust involves a comprehensive effort from individuals across an organization. Organizations that can inspire this type of trust will gain loyal customers today, while giving them the resources to transform medicine in the future.

Key Takeaways

To earn digital trust you must:

Think differently.

Build a culture where cybersecurity is a critical component for organizational success.

Plan differently.

Create a plan to bolster your data security as you plan for a future where consumer data is vital for healthcare decisions.

Act differently.

Take a proactive approach to cybersecurity by conducting thorough security testing and investing in marketing efforts to build your brand's reputation.

HURON

huronconsultinggroup.com